PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-236621
(43)Date of publication of application : 23.08.2002

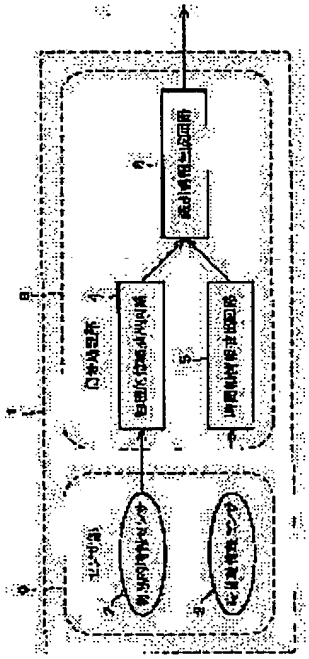
(51)Int.Cl. G06F 12/14
G11B 5/02
G11B 20/10

(21)Application number : 2001-032931
(22)Date of filing : 08.02.2001

(71)Applicant : SHARP CORP
(72)Inventor : KOJIMA KUNIO
KATAYAMA HIROYUKI
OTA KENJI

(54) SECURITY DEVICE, METHOD OF REGENERATING INFORMATION, METHOD OF RECORDING INFORMATION, METHOD OF PROTECTING INFORMATION, SYSTEM FOR RECORDING AND REGENERATING INFORMATION, AND METHOD OF DISTRIBUTING INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To protect information from being duplicated and being used illegally without permission of an information provider.
SOLUTION: Physical information characteristic to an individual information recording and regenerating device for conducting at least one out of recording and regeneration is detected by a physical information sensor 2, and identification information for identifying the information recording and regenerating device is generated by an identification information generating circuit 6, using the detected physical information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－236621
（P2002－236621A）
(43)公開日　平成14年８月23日(2002.8.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
Ｇ１１Ｂ　5/02		Ｇ１１Ｂ　5/02	Ｚ	５Ｄ０４４
20/10		20/10	Ｈ	５Ｄ０９１

審査請求　未請求　請求項の数16　ＯＬ　（全 27 頁）

(21)出願番号　特願2001－32931(P2001－32931)

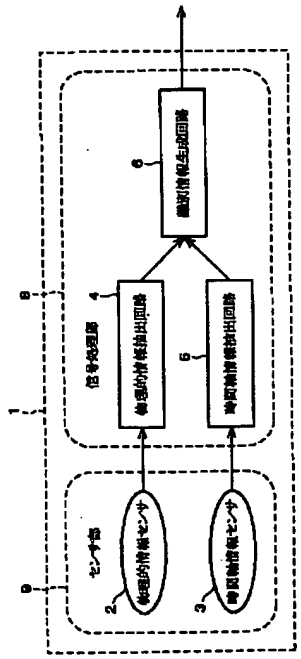
(22)出願日　平成13年２月８日(2001.2.8)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　小嶋　邦男
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(72)発明者　片山　博之
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100080034
弁理士　原　謙三

最終頁に続く

(54)【発明の名称】　セキュリティデバイス、情報再生方法、情報記録方法、情報保護方法、情報記録再生システムおよび情報配信方法

(57)【要約】
【課題】　情報の提供者に無断で情報が違法に複製され、不正に使用されることから情報を保護する。
【解決手段】　物理的情報センサ２により記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を検出し、検出された物理的情報を用いて、識別情報生成回路６により情報記録再生装置を識別するための識別情報を生成する。



1

【特許請求の範囲】

【請求項１】記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、

上記物理的情報検出手段により検出された物理的情報を用いて上記情報記録再生装置の識別情報を生成する識別情報生成手段とを備えていることを特徴とするセキュリティデバイス。

【請求項２】上記物理的情報を構成する物理量が、歪、漏洩磁場、電界、振動、加速度、圧力、音からなる群より選ばれる少なくとも一つであることを特徴とする請求項１に記載のセキュリティデバイス。

【請求項３】上記識別情報生成手段は、識別情報を生成するための情報として、

上記物理的情報検出手段により検出された物理的情報と、

上記情報記録再生装置に備えられた記録媒体を駆動する回転駆動手段から得られる情報とを用いることを特徴とする請求項１または２に記載のセキュリティデバイス。

【請求項４】上記識別情報生成手段は、識別情報を生成するための情報として、

上記物理的情報検出手段により検出された物理的情報と、

外部から任意に設定できるユーザ情報とを用いることを特徴とする請求項１、２または３に記載のセキュリティデバイス。

【請求項５】上記情報記録再生装置に加速度を与える印加部を備えていることを特徴とする請求項１ないし４のいずれか１項に記載のセキュリティデバイス。

【請求項６】記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を用いて生成された識別情報が付加された情報を再生する情報再生方法であって、

上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、

上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生することを特徴とする情報再生方法。

【請求項７】記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を用いて生成された識別情報により暗号化された情報を再生するにあたって、

上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行うことを特徴とする情報再生方法。

【請求項８】記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報記録方法において、

2

上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加し、

該識別情報が付加された情報を上記情報記録再生装置に記録することを特徴とする情報記録方法。

【請求項９】記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報記録方法において、

上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化し、

該暗号化された情報を上記情報記録再生装置に記録することを特徴とする情報記録方法。

【請求項１０】情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加し、

該識別情報が付加された情報を上記情報記録再生装置に記録し、

上記識別情報が付加された情報の再生にあたって、

上記識別情報が付加された情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、

上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生することを特徴とする情報保護方法。

【請求項１１】情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化し、

該暗号化された情報を上記情報記録再生装置に記録し、

上記暗号化された情報を再生するにあたって、

上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行うことを特徴とする情報保護方法。

【請求項１２】記録および再生の少なくとも一方を行う情報記録再生装置を含んでなる情報記録再生システムにおいて、

個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、

上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、

上記情報記録再生装置に記録すべき情報に上記識別情報を付加する識別情報付加手段と、

再生すべき情報に付加された識別情報と、該識別情報が付加された情報の再生に用いられる情報記録再生装置の識別情報とが一致するか否かを判断する判断手段とを備えてなることを特徴とする情報記録再生システム。

【請求項１３】記録および再生の少なくとも一方を行う情報記録再生装置を含んでなる情報記録再生システムにおいて、

個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、
上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、
情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化する暗号化手段と、
暗号化された情報を再生する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、該暗号化された情報を復号する復号手段とを備えてなることを特徴とする情報記録再生システム。
【請求項１４】上記識別情報生成手段は、識別情報を生成するための情報として、
上記物理的情報検出手段により検出された物理的情報と、
上記情報記録再生装置の装置仕様情報とを用いることを特徴とする請求項１２または１３に記載の情報記録再生システム。
【請求項１５】記録および再生の少なくとも一方を行う情報記録再生装置に情報を配信する情報配信方法において、
上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を配信すべき情報に付加し、
該識別情報が付加された情報を上記情報記録再生装置に配信することを特徴とする情報配信方法。
【請求項１６】記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報配信方法において、
上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて配信すべき情報を暗号化し、
該暗号化された情報を上記情報記録再生装置に配信することを特徴とする情報配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報の提供者に無断で情報が違法に複製され、不正に使用されることから情報を保護することを目的としたセキュリティデバイス、情報再生方法、情報記録方法、情報保護方法、情報記録再生システムおよび情報配信方法に関するものである。
【０００２】
【従来の技術】近年、デジタル情報をデジタルのままで容易に複製することができる記録媒体が開発され、デジタル情報の違法なコピーが容易に実行されるようになってきている。このため、デジタル化された音楽情報や映像情報等の著作権の保護、すなわちコンテンツの保護が重要な課題となっている。
【０００３】デジタル情報の著作権を保護するための技術としては様々な技術が開発されており、例えば、再生

専用媒体であるＤＶＤでは、強力なコピープロテクトを予め付加することにより違法コピーを防止している。
【０００４】また、特開２０００－１１２８２４号公報には、記録媒体の一つであるフラッシュメモリを用いたメモリシステムにおいて、著作権を保護するための技術が開示されている。上記公報に開示されたメモリシステムにおいては、通常の記録再生手段ではアクセスできないメモリ内部の領域にシステムの個別情報が保持されており、通常の情報は上記個別情報と関連付けて上記フラッシュメモリに記録・格納される。そして、記録・格納された情報を読み出す際には、当該情報と関連付けて記録・格納された個別情報と上記システムの個別情報との合致が確認される。すなわち、情報と関連付けて記録・格納された個別情報と上記システムの個別情報とが合致しない場合には、上記情報の読み出しが制限されることとなるため、単純に別のメモリシステムに情報をコピーしただけでは該情報を読み出すことは不可能となる。
【０００５】一方、特開２０００－２２８０６２号公報には、光ディスクシステムにおいて、光ディスクの製造時にディスク毎に異なるＩＤを記録しておくことが提案されている。上記ＩＤを暗号化された情報（コンテンツ）の復号鍵として利用することによりコンテンツの違法コピーを防止することができる。
【０００６】更に、特開２０００－４８４８２号公報には、情報記録媒体から読み出されたデジタル情報が特定の再生装置でしか再生できないようにすることにより、デジタル情報の不正使用を防止するシステムが開示されている。当該公報に開示されたシステムにおいては、再生装置のＩＤ情報を記録媒体の保護領域に記録しておくことにより、情報記録媒体から読み出されたデジタル情報を特定の再生装置でのみ再生可能とすることを実現している。
【０００７】
【発明が解決しようとする課題】しかしながら、既に提案されている上記システムは、いずれもあらかじめ記録媒体や情報記録再生装置等に仕掛けを設けることが必要であるため、現在世の中に出回っているパーソナルコンピュータ等のデジタル情報機器に既に組み込まれている情報記録媒体や、情報記録再生装置には適用することができないという問題点がある。例えば、デジタル情報の記録再生装置として多くのパーソナルコンピュータに組み込まれているハードディスクには、既に提案されている上記システムのいずれも適用することはできない。
【０００８】近年のデジタル情報機器において、ハードディスクの重要性はますます増加しており、ハードディスクはデジタル情報記録再生装置の主役に踊り出ている。今後、放送のデジタル化に伴い、従来のＶＴＲに替わってハードディスクを用いて情報の記録再生を行うデジタル情報機器が一般家庭にも入ってくる。更に、インターネットを利用したネット配信によるデジタル情報

（コンテンツ）の売買も急速に拡大することが予測されている。すなわち、デジタル情報を記録再生するための記録媒体としてのハードディスクの重要性は、今後ますます大きくなると考えられるが、ハードディスクを用いた情報の記録再生は無防備の状態で行われており、上述のようにハードディスクを用いた場合におけるコンテンツ保護を目的とした有用なシステムは未だ提案されていない。

【０００９】本発明は、上記の問題点を解決するためになされたものであり、ハードディスク等の既に市場に出回っている情報記録再生装置により、情報の記録および再生の少なくとも一方を行う場合における情報の保護に係わるものであり、現行のシステムに適応させることが可能なセキュリティデバイス、情報再生方法、情報記録方法、情報保護方法、情報記録再生システムおよび情報配信方法を提供することにある。

【００１０】

【課題を解決するための手段】本発明の発明者らは、これらの問題点を解決するために鋭意検討した結果、本発明に至ったものである。すなわち、情報を格納する情報記録再生装置の外部から、該情報記録再生装置に固有の物理的情報を検出し、該物理的情報を用いて個々の情報記録再生装置を識別すると共に、情報再生の許可／不許可を判断することを特徴としている。

【００１１】本発明のセキュリティデバイスは、上記の課題を解決するために、記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて上記情報記録再生装置の識別情報を生成する識別情報生成手段とを備えていることを特徴としている。

【００１２】上記の構成により、現行の情報記録再生装置本体の変更を必要とすることなく、個々の情報記録再生装置を識別することができる識別情報を容易に得ることが可能となる。

【００１３】すなわち、既に市場に出回っている情報記録再生装置は、それぞれに固有の物理的情報を有しているため、該物理的情報を用いて個々の情報記録再生装置を特定することができる。つまり、情報記録再生装置を構成する部品単体にはバラツキがあり、またこれらを組み立てる際には組立誤差が存在するため、情報記録再生装置からは、何らかの固有の物理的情報を検出することが可能である。このため、各種物理的情報の中でも固有の物理的情報を用いることにより、情報記録再生装置を識別するための識別情報を生成することができる。

【００１４】情報記録再生装置であるハードディスクドライブ（以下、ＨＤＤと略する）を例に挙げて、以下に説明する。ＨＤＤは、記録媒体である磁気ディスクとスピンドルモータとを含んで構成されており、磁気ディスクはスピンドルモータに固定されているため、磁気ディスクの重心とスピンドルモータの回転中心との相対的な関係は製造時点で決定され、ＨＤＤが破壊されるまでその相対的な関係は維持されることになる。また、磁気ディスクの重心とスピンドルモータの回転中心との相対的な関係（ズレ）は、磁気ディスクおよびスピンドルモータの単体のバラツキおよび組立誤差に影響され、ＨＤＤ毎に異なるものである。そして、両者の相対的な位置関係は、ＨＤＤ全体に対して力学的影響を与えるものであり、該力学的影響は、歪、振動、漏洩磁場、電界、圧力、音等の物理的情報として検出することができる。

【００１５】つまり、磁気ディスクの重心とスピンドルモータの回転中心との相対的な関係は破壊されるまで維持されるＨＤＤに固有の関係であり、その影響は物理的情報として検出することができる。したがって、ＨＤＤにおいては、磁気ディスク重心とスピンドルモータの回転中心との相対的な関係の影響を物理的情報として検出し、該物理的情報を用いて情報記録再生装置を識別する識別情報を生成することができる。

【００１６】また、ＨＤＤを構成する磁気ヘッドのアクチュエータを駆動する機構部は、永久磁石とボイスコイルにより構成されており、上記永久磁石の漏洩磁場は装置の外部においても検出可能であるため、上記アクチュエータの駆動電流を非接触に検出して物理的情報として用いることもできる。

【００１７】したがって、本発明のセキュリティデバイスは、既に市場に出回っているＨＤＤ等の情報記録再生装置に用いることができる。また、本発明のセキュリティデバイスにより、現行の情報記録再生装置の構成を変更することなく、該情報記録再生装置を識別する識別情報を得ることができる。

【００１８】本発明のセキュリティデバイスは、上記の課題を解決するために、上記物理的情報を構成する物理量が、歪、漏洩磁場、電界、振動、加速度、圧力、音からなる群より選ばれる少なくとも一つであることを特徴としている。

【００１９】上記の構成により、上記７種類の物理的情報の中から本発明の目的を達成するために適切な１種類ないし複数種類の組み合わせを選択することによって、情報記録再生装置を識別する識別情報をより確実に生成することができる。

【００２０】すなわち、情報記録再生装置のメカ（機構）部の個々のバラツキ、および組立誤差が情報記録再生装置に与える力学的影響は、歪、漏洩磁場、電界、振動、加速度、圧力、音として検出することができる。したがって、歪、漏洩磁場、電界、振動、加速度、圧力、音からなる群より選ばれる少なくとも一つの物理的情報を用いることにより、確実に識別情報を生成することができる。

【００２１】本発明のセキュリティデバイスは、上記の課題を解決するために、上記識別情報生成手段は、識別

情報を生成するための情報として、上記物理的情報検出手段により検出された物理的情報と、上記情報記録再生装置に備えられた記録媒体を駆動する回転駆動手段から得られる情報とを用いることを特徴としている。

【００２２】上記の構成により、上記識別情報生成手段により生成される識別情報の独立性を向上させることができる。

【００２３】すなわち、回転駆動手段から得られる情報から上記情報記録再生装置に備えられた記録媒体の回転情報を抽出して時間軸の情報を得ることができるため、上記物理的情報を時間軸の情報に関連させて識別情報を生成することができる。したがって、上記セキュリティデバイスの識別情報生成部により生成される識別情報の独立性が向上し、情報記録再生装置の識別をより確実に行うことができる。

【００２４】本発明のセキュリティデバイスは、上記の課題を解決するために、上記識別情報生成手段は、識別情報を生成するための情報として、上記物理的情報検出手段により検出された物理的情報と、外部から任意に設定できるユーザ情報とを用いることを特徴としている。

【００２５】上記の構成により、上記識別情報生成手段により生成される識別情報の独立性を向上させることができる。

【００２６】すなわち、上記識別情報を生成するために、上記物理的情報に加えて、ユーザ情報を用いることができる。これにより、例えば、同一の情報記録再生装置が複数のユーザにより使用される場合において、該情報記録再生装置を使用しているユーザ毎に、異なるユーザ情報を用いて識別情報を生成することが可能となる。このため、情報記録再生装置を使用しているユーザのそれぞれに対して異なる識別情報を作成することが可能となる。

【００２７】したがって、上記セキュリティデバイスの識別情報生成部により生成される識別情報の独立性が向上し、情報記録再生装置に加えて該識別装置を使用するユーザをも識別することができる。

【００２８】なお、本発明における「ユーザ情報」とは、ユーザを識別するために用いられる情報をいう。そして、ユーザ情報を設定する者としては、ユーザ、セキュリティデバイスの提供者、コンテンツ（情報）の著作権者等が挙げられる。

【００２９】本発明のセキュリティデバイスは、上記の課題を解決するために、上記情報記録再生装置に加速度を与える印加部を備えていることを特徴としている。

【００３０】上記の構成により、識別情報を生成するための物理的情報を再現性良く、確実に得ることができる。

【００３１】すなわち、上記印加部により、情報記録再生装置の筐体に加速度を与えて、その時の振動を物理的情報として検出することができる。加速度の付与により発生する振動は、情報記録再生装置の内部の状態と、筐体の取り付け状況により決定される。そして、メカ（機構）部の個々のバラツキ、および組立誤差により、情報記録再生装置内部の状態と、筐体の取り付け状況は、情報記録再生装置ごとに異なる。

【００３２】このため、上記印加部により、情報記録再生装置の筐体に加速度を加えて、その時の振動を物理的情報として検出することにより、情報記録再生装置の固有の物理的情報を確実に得ることができ、該物理的情報を用いて識別情報を生成することができる。したがって、情報記録再生装置を識別するための識別情報を確実に得ることができる。

【００３３】なお、上記印加部により与える加速度は、情報記録再生装置にダメージを与えず、情報の記録再生およびアクセス動作にも影響を与えない程度に調節されることはいうまでもない。

【００３４】本発明の情報再生方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を用いて生成された識別情報が付加された情報を再生する情報再生方法であって、上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生することを特徴としている。

【００３５】上記の構成により、識別情報により情報記録再生装置を特定して、情報の再生を行うことができるため、適法に情報の記録を行った情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が再生されることを防止することができる。

【００３６】すなわち、情報を記録する情報記録再生装置の物理的情報を用いて生成された識別情報が付加された情報を再生するにあたり、情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報と上記情報に付加されている識別情報とを比較することにより、情報が記録された情報記録再生装置と、情報を再生する情報記録再生装置とが一致するか否かを判断することができる。そして、上記判断結果により情報を再生するか否かを決定し、両者が一致した場合にのみ情報を再生し、一致しない場合は再生を行わないこととする。つまり、情報に付加された識別情報と、該情報の再生に用いられる情報記録再生装置の識別情報とを比較して情報の再生を行うか否かを決定することができる。

【００３７】本発明において、「識別情報が付加された情報」とは、識別情報と情報とが一括して記録されているものをいう。そして、該情報を再生する際には、識別情報と情報の読み取りが一括して実施されるが、該情報を再生する前に、該情報に付加されている識別情報の抽

出が行われる。そして、該抽出された識別情報と再生に用いられる情報再生装置の識別情報との比較、すなわち、識別情報の認識が行われた後に、情報を再生するか否かが決定されることとなる。

【0038】これにより、情報の記録に用いられた情報記録再生装置、および情報の再生に用いられる情報記録再生装置を特定することが可能となるため、両者を比較して違法コピーされた情報か否かを判断することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【0039】なお、本発明において「再生」とは、情報記録再生装置により情報の再生が行われ、該情報記録再生装置を使用する者等に情報が提供されることをいう。

【0040】本発明の情報再生方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う個々の情報記録再生装置に固有の物理的情報を用いて生成された識別情報により暗号化された情報を再生するにあたって、上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行うことを特徴としている。

【0041】上記の構成により、識別情報により情報記録再生装置を特定して、暗号化された情報を復号することができるため、適法に情報が記録された情報記録再生装置以外の情報記録再生装置に違法コピーされた情報を再生できないようにすることができる。

【0042】すなわち、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報により暗号化された情報を再生するにあたって、情報の再生に用いられる情報記録再生装置の物理的情報を用いて識別情報を生成し、該識別情報を復号鍵として使用して、上記暗号化情報の復号を行う。そして、復号に用いる識別情報と暗号化に用いられた識別情報とが一致する場合にのみ復号は成功し、暗号化される前の情報に復号されて、情報の再生を行うことができる。

【0043】これにより、暗号化の際に用いられた識別情報と、該情報の再生に用いられる情報記録再生装置の識別情報とが一致するか否かを確認した後に、情報を再生するか否かを決定することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【0044】本発明の情報記録方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報記録方法において、上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加し、該識別情報が付加された情報を上記情報記録再生装置に記録することを特徴としている。

【0045】上記の構成により、情報記録再生装置を識別する識別情報と記録すべき情報とを関連付けて情報の記録を行うことができる。

【0046】すなわち、情報を記録する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加することにより、記録すべき情報と、該情報を記録する情報記録再生装置とを関連付けることができる。

【0047】これにより、識別情報が付加された情報を再生するにあたって、該情報に付加された識別情報により、適法な情報の記録がなされた情報記録再生装置を特定することができるため、再生に用いられる情報記録再生装置と比較することが可能となる。このため、両者の比較により、再生すべき情報が違法コピーされた情報か否かを判断することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【0048】本発明の情報記録方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報記録方法において、上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化し、該暗号化された情報を上記情報記録再生装置に記録することを特徴としている。

【0049】上記の構成により、適法に情報が記録された情報記録再生装置の識別情報と記録すべき情報とを関連付けて情報の記録を行うことができる。

【0050】すなわち、情報を記録する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報を暗号鍵として使用して、上記情報を暗号化することができる。

【0051】これにより、暗号化された情報を再生するにあたって、再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、暗号化された情報を復号することが可能となる。そして、復号の際には、再生に用いられる情報記録再生装置の識別情報と、暗号化に用いられた識別情報とが一致する場合にのみ、暗号化された情報は復号される。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【0052】本発明の情報保護方法は、上記の課題を解決するために、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加し、該識別情報が付加された情報を上記情報記録再生装置に記録し、上記識別情報が付加された情報の再生にあたって、上記識別情報が付加された情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生することを特徴としている。

【００５３】上記の構成により、識別情報により情報記録再生装置を特定して、情報の記録および再生を行うことができるため、適法に情報の記録を行った情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が再生されることを防止することができる。

【００５４】すなわち、情報を記録する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加することにより、記録すべき情報と、該情報を記録する情報記録再生装置とを関連付けることができる。そして、識別情報が付加された情報の再生にあたって、情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報と上記情報に付加されている識別情報とを比較する。両者の比較により、情報が記録された情報記録再生装置と、情報を再生する情報記録再生装置とが一致するか否かを判断することができる。そして、上記判断結果により情報を再生するか否かを決定し、両者が一致した場合にのみ情報を再生し、一致しない場合は再生を行わないこととする。つまり、情報に付加された識別情報と、該情報の再生に用いられる情報記録再生装置の識別情報とを比較して、情報の再生を行うか否かを決定することができる。

【００５５】これにより、情報の記録に用いられた情報記録再生装置、および情報の再生に用いられる情報記録再生装置を特定し、両者を比較して違法コピーされた情報か否かを判断することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【００５６】本発明の情報保護方法は、上記の課題を解決するために、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化し、該暗号化された情報を上記情報記録再生装置に記録し、上記暗号化された情報を再生するにあたって、上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行うことを特徴としている。

【００５７】上記の構成により、識別情報により情報記録再生装置を特定して、情報の暗号化および復号を行うことができるため、適法に情報の記録を行った情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が復号されて、該復号された情報が再生されることを防止することができる。

【００５８】すなわち、情報を記録する際には、情報を記録する情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報を暗号鍵として使用して情報を暗号化して、暗号化された情報として上記情報記録再生装置に記録することにより、記録すべき情報と、該情報を記録する情報記録再生装置とを関連付けることができる。

【００５９】そして、暗号化された情報を再生するにあたって、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報を復号鍵として使用して、上記暗号化情報の復号を行う。復号に用いられた識別情報と暗号化に用いられた識別情報とが一致する場合にのみ復号は成功し、暗号化される前の再生可能な情報に復号されて、該情報が再生される。つまり、情報の再生に用いられる情報記録再生装置の識別情報と、情報の暗号化に用いられた識別情報とが一致する場合にのみ、暗号化された情報を復号して、再生することができる。

【００６０】これにより、情報の記録に用いられた情報記録再生装置、および情報の再生に用いられる情報記録再生装置を特定し、両者を比較して違法コピーされた情報か否かを判断することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【００６１】なお、本発明の情報再生方法、情報記録方法および情報保護方法は、上記セキュリティデバイスを利用して実施することができる。つまり、情報記録再生装置の識別情報として、上記セキュリティデバイスにより生成された情報を用いることができる。すなわち、上記セキュリティデバイスを利用して、情報記録再生装置において記録又は再生される情報を保護することができる。

【００６２】つまり、情報を記録する場合はセキュリティデバイスからの識別情報を記録すべき情報に関連させて記録し、再生する場合は再生情報がセキュリティデバイスからの識別情報に関連づけられているかどうかを確認することができる。

【００６３】これにより、情報記録再生装置を特定して再生が実行されることになり、正規に情報が記録された情報記録再生装置とは異なる他の情報記録再生装置に違法コピーされた情報は再生できないようにすることができる。

【００６４】本発明の情報記録再生システムは、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置を含んでなる情報記録再生システムにおいて、個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、上記情報記録再生装置に記録すべき情報に上記識別情報を付加する識別情報付加手段と、再生すべき情報に付加された識別情報と、該識別情報が付加された情報の再生に用いられる情報記録再生装置の識別情報とが一致するか否かを判断する判断手段とを備えてなることを特徴としている。

【００６５】上記の構成により、識別情報を用いて情報記録再生装置を特定して、情報の記録および再生を行う

ことができるため、適法な情報の記録がなされた情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が再生されることを防止することができる。

【0066】すなわち、上記物理的情報検出手段により検出された個々の情報記録再生装置に固有の物理的情報を用いて、上記識別情報生成手段は個々の情報記録再生装置を特定するための識別情報を生成することができる。このため、上記識別情報付加手段により、記録すべき情報に情報の記録に用いられる情報記録再生装置の識別情報を付加することにより、記録すべき情報と該情報を記録する情報記録再生装置とを関連付けることができる。そして、上記判断手段により、再生すべき情報に付加された識別情報と、該識別情報が付加された情報の再生に用いられる情報記録再生装置の識別情報とを比較し、情報の再生に用いられる情報記録再生装置の識別情報と、該情報の記録に用いられた情報記録再生装置とが一致するか否かを判断することができる。

【0067】これにより、情報の再生に用いられる情報記録再生装置および該情報の記録に用いられた情報記録再生装置を特定し、両者を比較して一致するか否かを判断することができるため、違法コピーされた情報の再生を防止することが可能となる。したがって、情報の不正使用を防止することにより情報を保護することができる。

【0068】なお、上記情報記録再生システムを構成する各手段の接続には、種々の接続手段を用いることができる。接続手段としては、例えば電話回線やインターネット等のネットワークを用いることができる。

【0069】本発明の情報記録再生システムは、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置を含んでなる情報記録再生システムにおいて、個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化する暗号化手段と、暗号化された情報を再生する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、該暗号化された情報を復号する復号手段とを備えてなることを特徴としている。

【0070】上記の構成により、識別情報を用いて情報記録再生装置を特定して、情報の暗号化および復号を行うことができるため、適法な情報の記録がなされた情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が再生されることを防止することができる。

【0071】すなわち、上記物理的情報検出手段により検出された個々の情報記録再生装置に固有の物理的情報を用いて、上記識別情報生成手段は個々の情報記録再生装置を特定するための識別情報を生成することができる。このため、上記暗号化手段により、情報の記録に用いられる情報記録再生装置の識別情報を用いて、記録すべき情報を暗号化することにより、該記録すべき情報と該情報を記録する情報記録再生装置とを関連付けることができる。そして、暗号化された情報は、上記復号手段により、暗号化された情報を再生する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて復号される。暗号化された情報の復号においては、復号に用いられる識別情報と暗号化に用いられた情報とが一致する場合にのみ暗号化される前の情報に復号されることとなる。

【0072】これにより、情報の再生に用いられる情報記録再生装置および該情報の記録に用いられた情報記録再生装置を特定し、両者を比較して一致するか否かを判断することができるため、違法コピーされた情報の再生を防止することが可能となる。したがって、情報の不正使用を防止することにより、情報を保護することができる。

【0073】本発明の情報記録再生システムは、上記の課題を解決するために、上記識別情報生成手段は、識別情報を生成するための情報として、上記物理的情報検出手段により検出された物理的情報と、上記情報記録再生装置の装置仕様情報とを用いることを特徴としている。

【0074】上記の構成により、情報記録再生装置本体の装置仕様情報を用いて識別情報を生成することができるため、より独立性の高い識別情報を生成することができる。

【0075】なお、本発明の情報記録再生システムは、上記セキュリティデバイスを物理的情報検出手段および識別情報生成手段として用いて実施することができるものであり、識別情報生成手段からの識別情報を既存のインターフェースを介してシステム本体に入力することができるため、現行のパーソナルコンピュータにも適応可能である。

【0076】また、識別情報が付加された情報を再生する時、情報保護機能により再生が不可能な場合は、それを明示する表示手段を備えていてもよい。これにより、ユーザは如何なる理由で情報の再生が実行されないのかを把握することができるし、情報提供者は情報の違法コピーに対する警告を与えることができる。

【0077】さらに、本情報記録再生システムは、セキュリティデバイスによる情報保護機能を停止又は解除することを指令できる保護機能停止解除手段を備えていてもよい。例えば、セキュリティデバイスが破損した場合や、記録されている情報にエラーが発生して正当な情報記録再生装置を用いても情報の再生が不可能となる事態に陥ることも充分に考えられる。こうした事態に備えるためには、強制的に情報保護機能を停止又は解除することが要求される。また、著作権者の許可の基に情報記録

再生装置の変更を実施する場合にも有益である。

【００７８】情報保護機能が停止又は解除された場合には、情報保護機能を再び稼動させることも必要である。この場合、再度、装置の識別情報に関連付けを行うことも可能としている。こうした特例の行為を実施できるユーザを限定しておくことは、情報記録再生システム全体の信頼性維持のために好ましい。

【００７９】また、情報記録再生装置であるＨＤＤ本体とシステム本体とのインターフェースを介してＨＤＤの仕様情報を入手することができるので、この仕様情報とセキュリティデバイスから得られる識別情報とから、より独立性の高い識別情報を生成することもできる。

【００８０】本発明の情報配信方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置に情報を配信する情報配信方法において、上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を配信すべき情報に付加し、該識別情報が付加された情報を上記情報記録再生装置に配信することを特徴としている。

【００８１】上記の構成により、情報が配信される情報記録再生装置の識別情報と、該情報記録再生装置に配信すべき情報とを関連付けることにより、保護機能を付加した情報として、情報を配信することができる。

【００８２】すなわち、配信する情報を格納する情報記録再生装置の識別情報を取得することにより該情報記録再生装置を特定することができる。そして、情報を配信する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加することにより、配信する情報と、該情報を記録する情報記録再生装置とを関連付けることができるため、配信する情報を再生することができる情報記録再生装置を制限することが可能となる。

【００８３】これにより、識別情報が付加された情報を再生するにあたって、該情報に付加された識別情報により、適法な情報の記録がなされた情報記録再生装置を特定することができるため、再生に用いられる情報記録再生装置と比較することが可能となる。このため、両者の比較により、再生すべき情報が違法コピーされた情報か否かを判断することができる。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【００８４】なお、配信された情報を再生する際に、該情報に付加された識別情報と、再生に用いられる情報記録再生装置の識別情報とが不一致の場合には、情報記録再生装置に格納されている配信された情報を消去するか、もしくはアクセスを不能とすることもできる。この場合は、両者の不一致が、連続で所定回数生じた場合のみ、消去やアクセス不能を実行することが好ましい。

【００８５】本発明の情報配信方法は、上記の課題を解決するために、記録および再生の少なくとも一方を行う情報記録再生装置に情報を記録する情報配信方法において、上記情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて配信すべき情報を暗号化し、該暗号化された情報を上記情報記録再生装置に配信することを特徴としている。

【００８６】上記の構成により、情報が配信される情報記録再生装置の識別情報と、配信すべき情報とを関連付けることにより、保護機能を付加した情報として、情報を配信することができる。

【００８７】すなわち、配信する情報を格納する情報記録再生装置の識別情報を取得することにより該情報記録再生装置を特定することができる。そして、情報を配信する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報を暗号鍵として使用して、上記情報を暗号化して配信することができる。

【００８８】これにより、暗号化された情報を再生するにあたって、再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、暗号化された情報を復号することが可能となる。そして、復号の際には、再生に用いられる情報記録再生装置の識別情報と、暗号化に用いられた識別情報とが一致する場合にのみ、暗号化された情報は復号される。したがって、不正に複製された情報が再生されることを防止して、情報を保護することが可能となる。

【００８９】暗号化された情報を再生するにあたって、情報が配信された情報記録再生装置とは異なる情報記録再生装置を用いて再生を行う場合には、暗号鍵と復号鍵とが一致せず、配信された暗号化された情報の復号が成功しない。この場合は、情報が不正に使用されていることとなるため、再生再生情報記録再生装置に格納されている、配信された情報を消去するか、もしくはアクセス不能状態とすることが好ましい。

【００９０】なお、本発明の情報配信方法は、上記セキュリティデバイスを用いた情報記録再生システムを利用して実施することができる。本発明の情報配信方法においては、情報提供者は、情報提供先であるユーザの情報記録再生装置の識別情報を予め入手し、それに基づいて配信する情報に保護機能を付加した後に、ユーザに配信するものである。

【００９１】配信する情報を格納する情報記録再生装置の識別情報を取得することにより該情報記録再生装置を特定することができるため、配信する情報と上記識別情報とを関連付けることにより、該情報に保護機能を付加することができる。つまり、情報に保護機能を付加した後に配信することにより、配信する情報を再生することができる情報記録再生装置を制限することが可能となる。

【００９２】なお、本発明の情報記録再生システムにおける情報のやりとりは、インターネットを介して行うこ

とにより、最も効率良く行うことができる。

【００９３】

【発明の実施の形態】以下、添付図面を参照して本発明の実施の形態を詳細に説明する。本発明は、情報記録再生装置の個々を識別するために装置固有の物理的情報を検出して、検出した物理的情報に基づいて識別情報を生成することを基本としている。発明の実施の形態は、識別情報を生成するセキュリティデバイス、情報再生方法、情報記録方法、情報保護方法、さらに情報保護を実現した情報記録再生システム、そしてそれを応用した情報配信方法にまで及ぶ。なお、以下の実施の形態は本発明の実施の形態を示した一例であり、本発明の技術的範囲を何ら限定するものではない。

【００９４】〔実施の形態１〕本発明の実施の一形態について図１ないし図１１に基づいて説明すれば、以下のとおりである。

【００９５】図１及び図２は、本発明の本実施の形態のセキュリティデバイスの概略の構成を示すブロック図である。図１に示すセキュリティデバイス１は、センサ部９と信号処理部（識別情報生成手段）８の２つに大きく別けられる。センサ部９は物理的情報センサ（物理的情報検出手段）２と時間軸情報センサ３とを備えて構成されており、信号処理部８は物理的情報抽出回路（識別情報生成手段）４と時間軸情報抽出回路５（識別情報生成手段）と識別情報抽出回路（識別情報生成手段）６とを備えて構成されている。

【００９６】物理的情報センサ２は物理的情報を検出するためのものであり、検出される物理量としては、例えば、歪、加速度、圧力、磁気、音響等が挙げられる。本実施の形態においては、物理的情報センサ２として歪センサを使用している。一方、時間軸情報センサ３は時間軸情報を得るためのものであり、装置の回転駆動系、具体的にはスピンドルモータの駆動電流の変化を電磁波の輻射から検出するものである。

【００９７】物理的情報センサ２から得られた物理的情報および時間軸情報センサ３から得られた時間軸情報は、信号処理部８へと導かれる。物理的情報センサ２からの物理的情報は、信号処理部８の物理的情報抽出回路４によりデジタル処理に適した形態の第１パルス信号に変換され、識別情報抽出回路６に入力される。具体的には、信号のピークを示す位置パルス、信号変化の最大となるポイントを示すマーカーパルス等が、第１パルス信号として生成される。時間軸情報センサ３からの時間軸情報は、信号処理部８の時間軸情報抽出回路５により、スピンドルモータの回転数に応じた時間パルスを示す第２パルス信号に変換されて、識別情報抽出回路６に入力される。

【００９８】上記のようにして得られた２つの信号（情報パルス）、すなわち第１パルス信号および第２パルス信号に基づいて、識別情報抽出回路６において識別情報が生成される。つまり、識別情報抽出回路６では、スピンドルモータの回転に応じた時間パルスと物理的情報から生成された第１パルス信号との位相関係を示す位相情報と、第２パルス信号から導かれる一回転の時間情報（回転周期情報）とを識別情報として出力する。なお、上記識別情報はデジタル情報として出力される。

【００９９】図２に示すセキュリティデバイス６１は、図１のセキュリティデバイス１に、さらに、ユーザ情報入力部７を備えて構成されている。上記ユーザ情報入力部７とは、外部から任意に設定して情報を入力することができるものであり、本実施の形態においては、ディップスイッチにより、デジタル情報を識別情報抽出回路６に、直接入力できるようにしている。セキュリティデバイス６１の識別情報抽出回路６から出力される識別情報には、上記位相情報と上記一回転の時間情報に加えて外部から設定されたユーザ情報が含まれる。これにより、生成される識別情報の独立性が向上し、識別情報として全く同じ情報が複数生成されることを防ぐことができる。

【０１００】図３はセキュリティデバイス１の外観を示したものである。同図に示すように、セキュリティデバイス１のセンサ部９と信号処理部８とは一体化されたチップとなっており、該チップにはユーザ情報入力部７としてのディップスイッチが搭載されている。信号処理部８の識別情報抽出回路６において生成された識別情報は、接続ケーブル１０を経由してコネクター１１からセキュリティデバイス１の外部に出力される。本実施例においては、接続ケーブル１０、コネクター１１のインターフェースとしてＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）のインターフェースを採用している。

【０１０１】つぎに、セキュリティデバイス１により、ハードディスクドライブ（以下、ＨＤＤと略する）等の情報記録再生装置の物理的情報が得られる原理について、図４～図８を用いて以下に説明する。

【０１０２】現行のＨＤＤ（情報記録再生装置）５２は、概略的には図４に示したように、筐体１２、スピンドルモータ（回転駆動手段）１３、制御回路基板１４、コネクター１５および磁気ディスク（記録媒体）１６を備えて構成されている。つまり、ＨＤＤ５２の筐体１２には、制御回路基板１４、および標準化されたインターフェースのコネクター１５が一体化されており、磁気ディスク１６はスピンドルモータ１３に固定されている。磁気ディスク１６とスピンドルモータ１３とのメカ（機構）的な関係は、ドライブの製造過程で決定されるものであり、磁気ディスク１６及びスピンドルモータ１３の単体のバラツキと組立誤差とによりＨＤＤに異なる。さらに、図４（ｂ）に示したように、磁気ディスク１６は、スピンドルモータ１３に複数枚搭載されるものであるため、両者のメカ的な関係はさらに複雑となる。

【０１０３】通常は、図５（ａ）に示すように、磁気デ

ィスク１６のディスク外径中心１７とディスク内径中心１８とは一致していない。また、両者が偶然に一致している場合においても、通常は、図５（ｂ）に示すようにスピンドル中心１９とディスク外径中心１７とは一致しないため、必ず磁気ディスク１６はスピンドル中心（回転中心）１９に対して偏心成分を有することになる。なお、上記スピンドル中心１９とはスピンドルモータ１３の回転中心のことをいう。

【０１０４】ＨＤＤ５２においては、記録媒体である磁気ディスク１６は取り外しが不可能な状態でスピンドルモータ１３に固定されているため、上記偏心成分が磁気ディスク１６に記録された情報の記録再生性能に影響を及ぼすことはほとんど無い。しかし、磁気ディスク１６が上記偏心成分を有することにより、磁気ディスク１６が高速で回転すると、磁気ディスク１６の回転に応じてＨＤＤ５２の筐体１２全体に振動が現れる。この振動は歪センサ、加速度センサ、磁気センサ、圧力センサ、音響センサ等のセンサにより検出することができるため、物理的情報として利用することが可能である。本実施の形態においては、歪センサを物理的情報センサ２として用いて上記振動を検知し、該検知した情報を物理的情報として用いている。

【０１０５】一方、スピンドルモータ１３としては、一般的に３相センサレスのＤＣモータが使用されている。上記ＤＣモーターは概略的に、図６に示したように３つの電気子２０を備えてなる構成である。そして、３つの電機子（回転駆動手段）２０のコイルに順番に駆動電流（Ｕ相、Ｖ相、Ｗ相）を流すことにより、上記ＤＣモーターは回転を維持することができる。Ｕ相、Ｖ相、Ｗ相の３つの駆動電流は、図７（ａ）に示したように位相をずらしながら、パルス形状で電機子２０のコイルに印加されている。そして、上記駆動電流は、電流の変化点においてはスパイクノイズとして外部から検出することができる。例えば、Ｕ相の駆動電流を図７（ａ）に示したパルス形状で電機子２０のコイルに印加した場合には、図７（ｂ）に示した波形のスパイクノイズとして検出することができる。すなわち、ＨＤＤ５２の外部から上記スパイクノイズを検出することにより磁気ディスク１６の回転情報（一回転の時間情報）を得ることが可能となる。

【０１０６】以上、説明したように、磁気ディスク１６（図５参照）が偏心成分を有することによりＨＤＤ５２の筐体１２（図４参照）に生ずる振動と、スピンドルモータ１３（図４参照）の回転時間情報とを組合せることにより、ＨＤＤ５２の個別的な識別を可能とする識別情報を生成することができる。

【０１０７】図８は物理的情報センサ２と時間軸情報センサ３（図１参照）とにより検出される生信号を示している。すなわち、同図には、物理的情報センサ２により検出された物理的情報と、時間軸情報センサ３により検出された時間軸情報（Ｕ相の駆動電流によるスパイクノイズの信号）とを示している。同図に示されたように、物理的情報は振動情報として得られ、時間軸情報はパルス情報として得られるものである。そこで、物理的情報は、物理的情報センサ２から信号処理部８に送出され、物理的情報抽出回路４において第１パルス信号に変換される。そして、時間軸情報は時間軸情報センサ３から信号処理部８に送出され、時間軸情報抽出回路５において第２パルス信号に変換される。上記の変換を行って第１パルス信号と第２パルス信号を得ることにより、図８に示すように両者の時間差△ｔを容易に求めることができるため、物理的情報と時間軸情報との位相関係を得ることができる。なお、本実施の形態においては、振動のピーク位置を示す位置パルスを第１パルス信号として用いている。

【０１０８】図１に示した信号処理部８において生成され、外部に出力される識別情報の一例を図９に示す。図９には、識別情報の一例として、ヘッダ情報とドライブ情報と一回転の時間情報と位相情報とユーザ情報とからなる識別情報を示している。図９に示した識別情報においては、先ずヘッダ情報が先頭に位置している。これは当該情報が識別情報であることを宣言するためのユニークなコードである。続いて、ドライブ種類情報があるが、これは種々のドライブを想定して導入しているものである。本実施例では、ＨＤＤを例として取り上げているが、例えば光ディスクドライブ等の他のドライブ装置においても本実施例と同様な手法によりデジタル情報のコンテンツの保護が可能であることから、導入しているものである。

【０１０９】続いて、磁気ディスク１６の回転数に相当する一回転の時間情報、磁気ディスク１６の回転と物理的情報との位相の関係についての位相情報、および外部から任意に設定できるユーザ情報となっている。図９に示したものは一例であり、例えば、これらの情報をスクランブルしたり、暗号化したりして記録しても良い。デジタル情報のコンテンツを保護するためには、種々の情報を用いて、上記識別情報の独立性を向上させることが重要である。

【０１１０】セキュリティデバイス６１（図２参照）を構成する時間軸情報センサ３及び時間軸情報抽出回路５の代わりに、加振部（印加部）２７及び加振部駆動部２８を備えたセキュリティデバイス７１を図１０に示す。ＨＤＤの物理的情報を得る方法としては、加振部２７によりＨＤＤに積極的に加速度を印加して、その時に発生する振動を物理的情報センサ２にて検出する方法も有効である。加速度の印加により発生する振動はＨＤＤの内部の状態と筐体の取り付け状況により決定されるため、上記方法により、それぞれのＨＤＤにおいて独立性の高い物理的情報を得ることができる。

【０１１１】加振部２７により加速度を与えるタイミン

グとしては、例えばセキュリティデバイス７１に電源が供給された時点において、自動的に実施しても良いし、ＨＤＤを有するコンピュータ等のシステムからの指令によって実施しても良い。また、与える加速度はＨＤＤにダメージを与えない程度であることは勿論のことであり、情報の記録再生およびアクセス動作にも影響を与えないように調整される。加振部２７としては、小型ソレノイド、超音波モータ等が適している。

【０１１２】更に、物理的情報を得るために、図示しない磁気ヘッドのアクチュエータを稼動する時に発生する振動または音を利用しても良い。この場合は、システム側から特別にアクセス動作を指示して、その時に発生する振動又は音を検出することが有効である。

【０１１３】セキュリティデバイス１をＨＤＤ５２の筐体１２に取り付けた状態を図１１に示している。同図のセキュリティデバイス１は、ＨＤＤ５２の物理的情報を検出するために、ＨＤＤ５２の筐体１２に直接密着するように取り付けられている。なお、セキュリティデバイス６１およびセキュリティデバイス７１も、セキュリティデバイス１と同様にＨＤＤ５２に対して取り付けることができる。

【０１１４】以上のように、セキュリティデバイスは、個々の情報記録再生装置に固有の物理的情報を用いて、情報記録再生装置を識別する識別情報を生成することができる。このため、現行の情報記録再生装置であるＨＤＤ本体の変更を必要とすることなく、個々のＨＤＤを識別することができる識別情報を容易に得ることができる。すなわち、上記識別情報を用いて情報記録再生装置と該情報記録再生装置により記録または再生される情報とを関連付けることにより、情報の不正な使用を防ぐことができる。

【０１１５】第１セキュリティデバイスは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報を検出し、情報記録再生装置を識別するための識別情報を生成するセキュリティデバイスとして構成されていてもよい。

【０１１６】上記の構成により、現行の情報記録再生装置本体の変更を必要とせずに個々の装置を識別する情報を容易に得ることができる。

【０１１７】上記第１セキュリティデバイスは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報として、歪、漏洩磁場、電界、振動、加速度、圧力、音の内、少なくとも一つを含むものであってもよい。

【０１１８】上記の構成により、情報記録再生装置内メカ部の個々のバラツキに起因する物理的情報を検出することができる。

【０１１９】上記第１セキュリティデバイスは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報と、前記情報記録再生装置に搭載されている回転駆動手段から得られる情報に基づいて、識別情報を生成するものであってもよい。

【０１２０】上記の構成により、回転駆動手段から情報記録媒体の回転情報を抽出することにより時間軸の情報が得られ、物理的情報を時間軸に関連させて識別情報を生成することができるため、独立性の高い識別情報を生成することができる。

【０１２１】上記第１セキュリティデバイスは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報と、外部から任意に設定できる情報に基づいて、識別情報を生成するものであってもよい。

【０１２２】上記の構成により、外部から任意に設定できる情報を用いて識別情報の独立性をさらに向上させることができる。

【０１２３】上記第１セキュリティデバイスは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報を検出する際に、前記情報記録再生装置に対して外部から加速度を与えるものであってもよい。

【０１２４】上記の構成により、外部から積極的に情報記録再生装置の筐体に加速度を加えて、その振動を物理的情報として検出することができる。

【０１２５】〔実施の形態２〕本発明の実施の他の一形態について図１２および図１３に基づいて説明すれば、以下のとおりである。

【０１２６】図１２および図１３は、本実施の形態の、情報再生方法、情報記録方法および情報保護方法を説明するブロック図を示している。いずれの図も情報記録再生装置において、情報を記録及び再生する状況を説明するものである。

【０１２７】本実施の形態では、情報が情報記録再生装置３１に記録される前に、識別情報付加手段３０において、当該情報に、セキュリティデバイス１から得られた情報記録再生装置３１の識別情報が自動的に付加される。すなわち、上記識別情報が付加された情報として情報記録再生装置３１に記録される。なお、識別情報付加手段３０における識別情報の付加は、使用者には認識されることなく実施される。そして、情報記録再生装置３１に記録された情報を再生するときには、認証手段（判断手段）３２において、当該情報に付加された識別情報と、セキュリティデバイス１から得られた情報記録再生装置３１の識別情報とが一致するか否かが判断される。

【０１２８】判断の結果、情報に付加された識別情報と、セキュリティデバイス１から得られた情報記録再生装置３１の識別情報とが一致した場合には、情報の再生処理は継続されて使用者は情報を利用することができる。しかし、両者が一致しない場合には、情報の再生処理は中断されることになる。

【０１２９】すなわち、情報の記録を行った情報記録再生装置を用いて情報を再生する場合には、該情報に付加

された識別情報とセキュリティデバイスから得られた情報記録再生装置の識別情報とが一致するため、情報を利用することができるが、異なる情報記録再生装置を用いて情報の再生を行う場合には、両者は一致しないため情報の再生は中断される。これにより、情報の記録を行った情報記録再生装置以外では、当該情報を再生することができなくなる。例えば、暗号化情報を違法コピーして他の情報記録再生装置に記録した場合には、該情報に付加された識別情報と、再生に用いられる情報記録再生装置の識別情報とが異なるため、情報の再生を実行できないこととなる。すなわち、情報を違法コピーして他の情報記録再生装置に記録した場合には、該情報の再生を行うことができないため、不正なコピーから情報を保護することができる。

【０１３０】ここで重要なポイントは、識別情報付加手段３０において情報に識別情報を付加する際に、情報に識別情報が既に付加されているか否かを判断し、既に識別情報が付加されている情報に対しては、新たな識別情報を付加しないようにすることである。すなわち、識別情報付加手段３０は、情報に識別情報を付加する前に、該情報が既に識別情報が付加された情報であるか否かについて判断し、該情報に識別情報が付加されている場合には識別情報の付加を行わず、該情報に識別情報が付加されていない場合に識別情報の付加を行う。これにより、情報の履歴が残るため、情報の保護を達成することができる。

【０１３１】セキュリティデバイス１から得られた情報記録再生装置３１の識別情報を暗号鍵として用いることにより、情報を保護する方法を説明するブロック図を図１３に示す。

【０１３２】まず、暗号化手段３３において情報を暗号化する際に、セキュリティデバイス１から得られた情報記録再生装置３１の識別情報が暗号鍵として用いられる。すなわち、記録すべき情報は、識別情報を暗号鍵として用いて暗号化された暗号化情報として情報記録再生装置３１に記録される。

【０１３３】情報記録再生装置３１には、情報を暗号化した暗号化情報が記録されているため、情報を再生するには暗号化情報を復号することが必要となる。当該復号は、復号手段３４において、セキュリティデバイス１から得られた情報記録再生装置３１の識別情報を復号鍵として用いて行われる。復号鍵が暗号鍵と一致する場合には復号が成功し、復号が成功して初めて使用者は情報を使用することができる。

【０１３４】つまり、使用者は、復号鍵として用いる識別情報が、暗号鍵として用いられた識別情報と一致する場合は情報を使用することができるが、両者が一致しない場合は情報を使用することができないこととなる。例えば、暗号化情報を違法コピーして他の情報記録再生装置に記録した場合には、復号鍵として用いられる識別情報は暗号鍵として用いられた識別情報と異なるため復号を実行できないこととなる。すなわち、暗号化情報を違法コピーして他の情報記録再生装置に記録しても復号鍵が異なるため、復号は実行できないことになり、情報の保護が達成される。

【０１３５】第１情報保護方法は、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報から、生成された情報記録再生装置の識別情報を用いて、前記情報記録再生装置に記録されている情報を保護する情報保護方法であってもよい。

【０１３６】上記第１情報保護方法は、情報を記録する際には、情報記録再生装置の物理的情報から生成された識別情報を記録すべき情報に付加し、情報を再生する際には、再生する情報に付加されている識別情報と情報記録再生装置の識別情報が一致しているかどうかを判断し、一致している場合は情報の再生を実行し、一致しない場合は情報の再生を実行しないものであってもよい。

【０１３７】上記第１情報保護方法は、情報を記録する際には、情報記録再生装置の物理的情報から生成された識別情報を使用して、記録すべき情報を暗号化し、情報を再生する際には、情報記録再生装置の識別情報により再生する情報を復号するものであってもよい。

【０１３８】上記の構成により、情報を記録する場合はセキュリティデバイスからの識別情報を記録すべき情報に関連させて記録し、情報を再生する場合は再生される情報がセキュリティデバイスからの識別情報に関連付けられているかどうかを確認することができる。これにより、情報記録再生装置を特定して再生が実行されることになり、他の情報記録再生装置に違法コピーされた情報は再生できないようにすることができる。

【０１３９】〔実施の形態３〕本発明の実施のさらに他の一形態について図１４および図１５に基づいて説明すれば、以下のとおりである。

【０１４０】セキュリティデバイス１を装着した情報記録再生装置３１が内蔵された情報機器３５の概略を図１４に示している。本実施の形態の情報記録再生システムは、セキュリティデバイス１と情報記録再生装置３１と情報機器３５とディスプレイ３８とキーボード３９とマウス４０とを備えて構成されている。情報機器３５は、デジタル情報を外部から入力できるインターフェースとして、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）コネクター３６およびＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）アダプタ３７を備えており、セキュリティデバイス１が取り付けられた情報記録再生装置３１を内蔵している。また、情報機器３５としては、例えばパーソナルコンピュータ（以下、ＰＣと略する）等が用いられる。

【０１４１】本実施の形態の情報記録再生システムにおいては、情報記録再生装置３１の識別情報は、セキュリティデバイス１により検出されて、ＵＳＢコネクター３

６を介して情報機器３５に取り込まれる構成となっている。現在、ＵＳＢはＰＣ等の情報機器に広く採用されいるため、本実施の形態の識別情報をＵＳＢコネクター３６を介して情報機器３５に取り込む構成は、既存のＰＣ等の情報機器に適用することが可能である。また、識別情報を情報機器３５に取り込む際のインターフェースとしては、ＵＳＢコネクター３６以外に、シリアルインターフェース、パラレルインターフェース、ＬＡＮアダプタ等をも用いることができる。つまり、識別情報を情報機器３５に取り込む際のインターフェースとしては、デジタル情報を外部から入力することが可能なものであればよい。

【０１４２】上記のように、情報機器３５は、セキュリティデバイス１から、情報記録再生装置３１の識別情報を得ることができるため、該識別情報を用いて情報の保護を実現することができる。当該情報の保護を実現する方法としては、具体的には、本発明の実施の形態２の情報保護方法を挙げることができる。そして、情報記録再生装置３１によって情報を再生又は使用する際に、情報記録再生システムの情報保護機能が働いて情報の再生又は使用が不可能な状況になったときには、ディスプレイ３８上にその旨を表示して警告することが重要である。これにより、不正にコピーした情報の使用者に対して、当該情報の使用についての警告を与えることができる。なお、上記情報記録再生システムの情報保護機能が働く場合としては、例えば再生または使用する情報が、不正にコピーされたものである場合が該当する。

【０１４３】また、本実施の形態の情報記録再生システムは、情報保護機能そのものを停止もしくは解除することも可能である。具体的には、情報保護機能を停止するためのコマンドをあらかじめ準備しておき、必要な場合には、キーボード３９又はマウス４０を用いて当該コマンドを実行することにより、情報保護機能の停止もしくは解除を実行できるようにしている。

【０１４４】上記必要な場合とは、具体的には、情報記録再生装置３１の破損により情報記録再生装置３１を変更しなければならない状況が発生した場合や、情報記録再生装置３１に記録された情報へのアクセスが必要となる緊急事態が発生した場合等を挙げることができる。

【０１４５】また、本実施の形態の情報記録再生システムは、異常事態、即ち情報保護機能そのものを停止、若しくは解除することが必要な事態が解消された場合には、再度、情報保護機能を開始するコマンドも備えており、該コマンドの実行により、情報保護機能を再度開始することができる。ここで、システム全体の信頼性のためには、情報保護機能の停止もしくは解除、または再開を実行できる使用者を特定の者に限定しておくことが好ましい。

【０１４６】上記情報機器３５（図１４参照）に内蔵された情報記録再生装置３１としてＨＤＤ５２を用いた場合において、ＨＤＤ５２の個別化を更に押し進める方法を説明するブロック図を図１５に示す。ＰＣ等の情報機器３５を構成するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）４３は、ＨＤＤ５２の装置仕様情報をＩＤＥ（Ｉｎｔｅｇｒａｔｅｄ Ｄｅｖｉｃｅ Ｅｌｅｃｔｒｏｎｉｃｓ）４１を介して入手することができる。当該装置仕様情報としては、具体的には、ＨＤＤ５２のセクタ数、シリンダ数、ヘッド数等が挙げられる。つまり、ＣＰＵ４３は、ＨＤＤ５２の識別情報をセキュリティデバイス１からＵＳＢコネクター３６を介して得ることができ、さらに、ＨＤＤ５２の装置仕様情報をＩＤＥ４１を介して得ることができる。

【０１４７】従って、ＨＤＤ５２の識別情報を生成する際に、識別情報および装置仕様情報を用いることができる。これにより、識別情報と装置仕様情報とを組み合わせることにより、いずれか一方の情報に基づくよりも更に独立性の高い識別情報を生成することが可能となる。

【０１４８】第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段とを備えた情報記録再生システムとして構成されていてもよい。

【０１４９】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報に基づいて記録された情報を保護する機能とを備えたものであってもよい。

【０１５０】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報を記録すべき情報に付加する手段と、再生すべき情報に付加された識別情報と前記情報記録再生装置の識別情報が一致するかどうかを判断する手段とを備えたものであってもよい。

【０１５１】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報を使用して記録すべき情報を暗号化する手段と、再生すべき情報を前記情報記録再生装置の識別情報により復号する手段とを備えたものであってもよい。

【０１５２】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生

システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報に基づいて記録された情報を保護する機能と、情報の再生が実行できない場合は、それを明示する機能を備えたものであってもよい。

【０１５３】上記の構成により、ユーザは如何なる理由で再生が実行されないのかを把握することができるし、違法コピーに対する警告を与えることができる。

【０１５４】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報に基づいて記録された情報を保護する機能とを備えた情報記録再生システムであって、記録された情報を保護する機能を停止又は解除および稼動することを指令する手段を備えたものであってもよい。

【０１５５】上記の構成により、例えば、セキュリティデバイスが破損した場合や、情報にエラーが発生して正当な装置でも再生が不可能となる事態が発生した場合においても、強制的に情報保護機能の停止または解除をすることができる。また、著作権者の許可の基に情報記録再生装置の変更を行う場合にも有益である。

【０１５６】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生装置の、物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段と、生成された識別情報に基づいて記録された情報を保護する機能とを、備えた情報記録再生システムにおいて、特定の使用者が記録された情報を保護する機能を停止又は解除および稼動することを実行できるものであってもよい。

【０１５７】上記の構成により、情報を保護する機能を停止または解除および稼働することを実行できる者を特定の使用者（ユーザ）に限定することができるため、システム全体の信頼性を維持することができる。

【０１５８】上記第１情報記録再生システムは、情報を記録又は再生もしくは記録再生を実行する情報記録再生システムにおいて、情報記録再生装置の物理的情報を検出する手段と、検出された物理的情報から情報記録再生装置を識別するための識別情報を生成する手段とを備え、情報記録再生装置の装置仕様情報を得て、前記識別情報とともに情報記録再生装置を個別化するものであってもよい。

【０１５９】上記の構成により、情報記録再生装置から得られる仕様情報とを識別情報の生成に用いることができるため、より独立性の高い識別情報を生成することができる。

【０１６０】〔実施の形態４〕本発明の実施の他の一形態について図１６ないし図２０に基づいて説明すれば、以下のとおりである。本実施の形態においては、セキュリティデバイスを装着した情報記録再生システムを用いた情報配信方法として、本発明を実施した場合について説明する。

【０１６１】本実施の形態の情報配信方法に用いられる情報記録再生システムの概略の構成を示すブロック図を図１６に示す。上記情報記録再生システムは、第１サーバシステム４４と第１ユーザシステム４５とから構成されており、両者はネットワークを介して接続されている。上記のネットワークは、公衆電話回線やその他の高速通信回線、ならびにそれらの回線間のインターネット回線等により構成されている。第１サーバシステム４４は、概略的に識別情報付加手段３０と情報記憶手段４８とを備えてなっており、第１ユーザシステム４５は、概略的にセキュリティデバイス１と情報記録再生装置３１と認証手段３２とを備えてなっている。

【０１６２】つづいて、上記情報記録再生システムを用いて行われる情報提供方法について、図１７を用いて説明する。

【０１６３】まず、第１サーバシステム４４に対して、第１ユーザシステム４５から情報の提供が要求される（Ｓ１１）。続いて、第１ユーザシステム４５からの情報提供の要求に応じて、第１サーバシステム４４から、情報を格納する第１ユーザシステム４５の情報記録再生装置３１の第１識別情報が要求される（Ｓ１２）。当該要求に応じて、セキュリティデバイス１は、情報記録再生装置３１の物理的情報に基づいて作成した第１識別情報（識別情報）を第１サーバシステム４４に出力する（Ｓ１３）。なお、本実施の形態においては、セキュリティデバイスからサーバシステムに出力される識別情報を第１識別情報という。

【０１６４】本実施の形態においては、第１ユーザシステム４５は、第１サーバシステム４４の要求に応じて第１識別情報を出力しているが、第１サーバシステム４４から要求される前に出力してもよい。例えば、第１ユーザシステム４５は、情報提供を要求する際に第１識別情報を出力してもよい。

【０１６５】第１サーバシステム４４は、セキュリティデバイス１から出力された第１識別情報を、ネットワークを介して得る（Ｓ１４）。なお、第１ユーザシステム４５からの情報提供の要求の際に、第１識別情報が第１サーバシステム４４に出力されている場合には、第１サーバシステム４４は情報提供の要求と第１識別情報とを同時に得ることとなる。

【０１６６】第１サーバシステム４４は、識別情報付加手段３０により、提供する情報に第１ユーザシステム４５から入手した第１識別情報を付加する（Ｓ１５）。そして、その後に、第１サーバシステム４４は、第１識別情報が付加された情報を第１ユーザシステム４５に対し

て配信する（Ｓ１６）。第１ユーザシステム４５は、配信された情報をそのまま情報記録再生装置３１に格納する（Ｓ１７）。

【０１６７】ユーザが情報を再生する場合、すなわち第１ユーザシステム４５において、配信された情報の再生要求がなされる（Ｓ１８）と、認証手段３２は、情報記録再生装置３１に格納された情報を読み出し、該情報に付加されている第１識別情報と、セキュリティデバイス１から得られた情報記録再生装置３１の第２識別情報とが一致するか否かの判断を行う（Ｓ１９）。両者が一致したときは、再生処理は継続されて、第１ユーザシステム４５において、情報が再生される（Ｓ２１）、すなわち、ユーザは情報を使用することができる。しかし両者が一致しないときは再生処理は中断される（Ｓ２２）。すなわち、ユーザは情報を使用することができない。なお、本実施の形態においては、セキュリティデバイスからユーザシステムに出力される識別情報を第２識別情報という。

【０１６８】Ｓ１９において、情報の再生処理の際にセキュリティデバイス１から得られた第２識別情報と、情報に付加されている第１識別情報とが一致しない場合は、情報記録再生装置３１に記録されている情報は正当性を有しない情報、すなわち、不法にコピーされた情報ということになる。

【０１６９】したがって、上記情報を情報記録再生装置３１から削除をする処理を行うことは、該情報を保護するために有益である。あるいは、これ以後は、当該情報に対してアクセスできないようにすることも好ましい。上記アクセスの制限は、具体的には、情報記録再生装置３１の情報が記録されている領域において、不良セクタ等の設定を実施する方法により行うことができる。更に、例えば、測定誤差等の予測できない理由により第１識別情報と第２識別情報との不一致が生じることも考えられるため、両者が一致しない状態が連続して所定回数起きた場合に限定して、上記削除やアクセスを制限する処理を実施することとしてもよい。

【０１７０】本実施の形態の情報配信方法に用いられる情報記録再生システムは、図１８に示すように、ネットワークを介して接続されている第２サーバシステム５４と第２ユーザシステム５５とから構成されていてもよい。第２サーバシステム５４は、概略的に暗号化手段３３と情報記憶手段４８とを備えてなっており、第１ユーザシステム４５は、概略的にセキュリティデバイス１と情報記録再生装置３１と復号手段３４とを備えてなっている。

【０１７１】つづいて、上記情報記録再生システムを用いて行われる情報提供方法について、図１９を用いて説明する。

【０１７２】まず、第２サーバシステム５４に対して、第２ユーザシステム５５から情報の提供が要求される

（Ｓ３１）。続いて、第２ユーザシステム５５からの情報提供の要求に応じて、第２サーバシステム５４から、第２ユーザシステム５５の情報を格納する情報記録再生装置３１の第１識別情報が要求される（Ｓ３２）。当該要求に応じて、セキュリティデバイス１は、情報記録再生装置３１の物理的情報に基づいて作成した第１識別情報を第２サーバシステム５４に出力する（Ｓ３３）。

【０１７３】第２サーバシステム５４は、セキュリティデバイス１から出力された第１識別情報をネットワークを介して得る（Ｓ３４）。続いて、第２サーバシステム５４は、上記第１識別情報を暗号鍵として、暗号化手段３３により情報を暗号化する（Ｓ３５）。そして、その後に、第２サーバシステム５４は、暗号化した情報である暗号化情報を第２ユーザシステム５５に配信する（Ｓ３６）。第２ユーザシステム５５は、配信された暗号化情報をそのまま情報記録再生装置３１に格納する（Ｓ３７）。

【０１７４】ユーザが情報を再生する場合、すなわち第２ユーザシステム５５において、配信された情報の再生要求がなされる（Ｓ３８）と、復号手段３４は、情報記録再生装置３１に格納された暗号化情報を読み出し、セキュリティデバイス１から得られた情報記録再生装置３１の第２識別情報を復号鍵として復号を行う（Ｓ３９）。復号鍵として用いる第２識別情報と、暗号鍵として用いた第１識別情報とが一致したときは、復号が正常に実施される。すなわち、暗号化情報は復号され、第２ユーザシステム５５において、正常に復号された情報が再生される（Ｓ４１）。つまり、ユーザは情報を使用することができる。しかし、第１識別情報と第２識別情報とが一致しない場合、すなわち、暗号鍵と復号鍵とが一致しない場合は、復号は失敗するため、第２ユーザシステム５５において正常に復号された情報を再生することは不可能であり、再生処理は中断される（Ｓ４２）。つまり、ユーザは情報を使用することができない。

【０１７５】Ｓ３９において、暗号化情報の復号処理の際に復号鍵と暗号鍵とが一致しない場合、すなわち、セキュリティデバイス１から得られた第２識別情報と、情報の暗号化に用いられた第１識別情報とが一致しない場合は、情報記録再生装置３１に記録されている暗号化情報は正当性を有しない情報、すなわち、不法にコピーされた情報ということになる。

【０１７６】したがって、上記情報を暗号化情報を情報記録再生装置３１から削除する処理を行うことは、該情報を保護するために有益である。あるいは、これ以後は、当該情報に対してアクセスできないようにすることも好ましい。当該アクセスの制限は、具体的には、情報記録再生装置３１の暗号化情報が記録されている領域において、不良セクタ等の設定を実施する方法により行うことができる。更に、例えば、測定誤差等の予測できない理由により、第１識別情報識別情報と第２識別情報と

の不一致が生じることも考えられるため、両者が一致しない状態が連続して所定回数起きた場合に限定して上記の削除やアクセスの制限等の処理を実施することとしてもよい。

【0177】ユーザシステムが複数の情報記録再生装置を含んで構成されている場合について、図20を用いて説明する。同図に示すように、第3ユーザシステム65は、第1情報記録再生装置46と第2情報記録再生装置47の2つの情報記録再生装置を含んで構成されている。

【0178】第1サーバシステム44は、第3ユーザシステム65からの要求により情報を配信する場合、第3ユーザシステム65が1つのライセンスのみを有する状況においては、第3ユーザシステム65の第1情報記録再生装置46または第2情報記録再生装置47のいずれかについて第1識別情報を入手し、それに基づいて情報情報に第1識別情報を付加して配信することになる。

【0179】第3ユーザシステム65では、第1サーバシステム44に出力された第1識別情報が検出された情報記録再生装置に、配信された情報を格納する。そして、情報が格納された以降は、情報を格納した情報記録再生装置においてのみ、該情報を使用することができる。

【0180】つまり、第1サーバシステム44は第3ユーザシステム65を構成する複数の情報記録再生装置のうちのいずれか一つを特定して、情報を配信することになる。このため、ユーザは、勝手に複数の情報記録再生装置に情報を格納することはできない。また、情報を格納した情報記録再生装置から他の情報記録再生装置に違法コピーがなされた場合は、配信された情報に付加された第1識別情報と、再生する際に確認される第2識別情報とが異なるために再生は中断され、情報を使用することはできない。

【0181】勿論、第3ユーザシステム65にたいして2つのライセンスが与えられる場合においては、第1サーバシステム44は2つの情報記録再生装置のそれぞれについて第1識別情報を入手し、情報記録再生装置それぞれの第1識別情報を付加した情報を配信することとなる。そして、第3ユーザシステム65は、それぞれの情報記録再生装置に配信された情報を格納することができる。これにより、第3ユーザシステム65では、いずれの情報記録再生装置に格納された情報も使用することが可能となる。なお、本実施の形態においては、ユーザシステムを構成する情報記録再生装置の数、およびユーザシステム65に与えられるライセンス数を、1または2とした場合について説明したが、これに限られるものではなく、いずれも任意の数とすることができる。

【0182】以上のように、サーバシステムが、ライセンス数に応じて情報記録再生装置の第1識別情報を取得し、該第1識別情報を付した情報を配信することにより、ライセンス数に応じた情報記録媒体において、配信された情報を利用することが可能となる。

【0183】以上詳述したように、本発明は個々の情報記録再生装置に固有の物理的情報を検出して、その物理的情報を基に情報記録再生装置を個別化するための識別情報を生成することを特徴としている。

【0184】識別情報を生成するセキュリティデバイスを現行の情報記録再生装置に対して適用することで、個々の装置を識別することが可能となり、記録される情報の保護機能を付加することが容易に実現できる。この保護機能により、特定の情報記録再生装置においてのみ情報の再生が許可されるという環境を提供できる。従って、情報の著作権保護が特に重要視される情報配信方法において、効果的な保護が実現できる。

【0185】第1情報配信方法は、情報を利用者に対して配信する情報配信方法において、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づいて配信情報に保護機能を付加して配信する情報配信方法であってもよい。

【0186】上記第1情報配信方法は、情報を利用者に対して配信する情報配信方法において、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報を配信情報に付加して配信するものであってもよい。

【0187】上記第1情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報を配信情報に付加して配信する情報配信方法において、利用者が情報記録再生装置に記録された配信情報を再生する場合、配信情報に付加された識別情報と利用者の情報記録再生装置の識別情報が一致することを判断した後に再生が実行されるものであってもよい。

【0188】上記第1情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報を配信情報に付加して配信する情報配信方法において、利用者が情報記録再生装置に記録された配信情報を再生する場合、配信情報に付加された識別情報と利用者の情報記録再生装置の識別情報が一致しない時は記録された配信情報を消去もしくはアクセス不能の状態にするものであってもよい。

【0189】上記第1情報配信方法は、情報を利用者に対して配信する情報配信方法において、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づいて配信情報を暗号化して配信するものであってもよい。

【0190】上記第1情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づき配信情報を暗号化して配信する情報配信方法において、利用者が情報記録再生装置に記録された配信情報を再生する場合、暗号化された配信情報を利用者の情報記録再生装置の識別情報により復号してた後に再生が実行されるものであってもよい。

【０１９１】上記第１情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づき配信情報を暗号化して配信する情報配信方法において、利用者が情報記録再生装置に記録された配信情報を再生する場合、暗号化された配信情報を利用者の情報記録再生装置の識別情報により復号が不可能であった時は、記録された配信情報を消去もしくはアクセス不能の状態にするものであってもよい。

【０１９２】上記第１情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づき保護機能を付加して情報を配信する情報配信方法において、前記識別情報は、前記情報記録再生装置の物理的情報から生成されたものであってもよい。

【０１９３】上記第１情報配信方法は、配信先の情報記録再生装置の識別情報を予め取得し、取得した識別情報に基づき保護機能を付加して情報を配信する情報配信方法において、インターネットを介して配信するものであってもよい。

【０１９４】これにより、情報のやりとり（送受信）を効率的に行うことができる。

【０１９５】

【発明の効果】本発明のセキュリティデバイスは、以上のように、個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて上記情報記録再生装置の識別情報を生成する識別情報生成手段とを備えた構成である。

【０１９６】それゆえ、個々の情報記録再生装置に固有の物理的情報を用いて、情報記録再生装置を識別する識別情報を生成することができる。これにより、現行の情報記録再生装置本体の変更を必要とすることなく、個々の情報記録再生装置を識別することができる識別情報を容易に得ることができるという効果を奏する。

【０１９７】本発明のセキュリティデバイスは、以上のように、上記物理的情報を構成する物理量が、歪、漏洩磁場、電界、振動、加速度、圧力、音からなる群より選ばれる少なくとも一つである構成である。

【０１９８】それゆえ、上記７種類の物理的情報の中から本発明の目的を達成するために適切な１種類ないし複数種類の組み合わせを選択することができる。これにより、情報記録再生装置を識別する識別情報をより確実に生成することができるという効果を奏する。

【０１９９】本発明のセキュリティデバイスは、以上のように、上記識別情報生成手段は、識別情報を生成するための情報として、物理的情報と、上記情報記録再生装置に備えられた記録媒体を駆動する回転駆動手段から得られる情報とを用いる構成である。

【０２００】それゆえ、回転駆動手段から得られる情報から上記情報記録再生装置に備えられた記録媒体の回転情報を抽出して時間軸の情報を得ることができるため、上記物理的情報を時間軸の情報に関連させて識別情報を生成することができる。これにより、上記識別情報生成手段により生成される識別情報の独立性を向上させることができるという効果を奏する。

【０２０１】本発明のセキュリティデバイスは、以上のように、上記識別情報生成手段は、識別情報を生成するための情報として、物理的情報と、外部から任意に設定できるユーザ情報とを用いる構成である。

【０２０２】それゆえ、物理的情報に加えてユーザ情報を用いて識別情報を生成することができる。これにより、識別情報の独立性が向上し、情報記録再生装置に加えて該識別装置を使用するユーザをも識別することができるという効果を奏する。

【０２０３】本発明のセキュリティデバイスは、以上のように、上記情報記録再生装置に加速度を与える印加部を備えた構成である。

【０２０４】それゆえ、印加部により、情報記録再生装置の筐体に加速度を与えて、その時の振動を物理的情報として検出することができる。これにより、識別情報を生成するための物理的情報を再現性良く、確実に得ることができるという効果を奏する。

【０２０５】本発明の情報再生方法は、以上のように、情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生する構成である。

【０２０６】それゆえ、識別情報により情報記録再生装置を特定して、情報の再生を行うことができる。これにより、違法にコピーされた情報が再生されることを防止できるため、不正な使用から情報を保護することができるという効果を奏する。

【０２０７】本発明の情報再生方法は、以上のように、個々の情報記録再生装置に固有の物理的情報を用いて生成された識別情報により暗号化された情報を再生するにあたって、上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行う構成である。

【０２０８】それゆえ、識別情報により情報記録再生装置を特定して、暗号化された情報を復号することができる。これにより、違法にコピーされた情報が再生されることを防止できるため、不正な使用を防止して情報を保護することができるという効果を奏する。

【０２０９】本発明の情報記録方法は、以上のように、情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加する構成である。

【０２１０】それゆえ、情報記録再生装置を識別する識別情報と記録すべき情報とを関連付けることができる。

このため、識別情報が付加された情報を再生するにあたって、該情報に付加された識別情報により、適法な情報の記録がなされた情報記録再生装置を特定することができるため、不正に複製された情報が再生されることを防止して、不正な使用を防止して情報を保護することができるという効果を奏する。

【0211】本発明の情報記録方法は、以上のように、情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化する構成である。

【0212】それゆえ、情報記録再生装置の識別情報と記録すべき情報とを関連付けて情報の記録を行うことができる。このため、不正に複製された情報が再生されることを防止して、不正な使用を防止して情報を保護することができるという効果を奏する。

【0213】本発明の情報保護方法は、以上のように、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を記録すべき情報に付加し、該識別情報が付加された情報を上記情報記録再生装置に記録し、上記識別情報が付加された情報の再生にあたって、上記識別情報が付加された情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、上記情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報と、該情報に付加された識別情報とを比較し、両者が一致した場合にのみ上記情報を再生する構成である。

【0214】それゆえ、識別情報により情報記録再生装置を特定して、情報の記録および再生を行うことができる。このため、適法に情報の記録を行った情報記録再生装置以外の情報記録再生装置に違法にコピーされた情報が再生されることを防止することができるため、不正な使用を防止して情報を保護することができるという効果を奏する。

【0215】本発明の情報保護方法は、以上のように、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化し、該暗号化された情報を上記情報記録再生装置に記録し、上記暗号化された情報を再生するにあたって、上記暗号化された情報を、該情報の再生に用いられる情報記録再生装置に固有の物理的情報を用いて生成された識別情報により復号し、復号が成功した場合にのみ情報の再生を行う構成である。

【0216】それゆえ、識別情報により情報記録再生装置を特定して、情報の暗号化および復号を行うことができる。これにより、違法にコピーされた情報が復号されて、該復号された情報が再生されることを防止することができるため、不正な使用を防止して情報を保護することができるという効果を奏する。

【0217】本発明の情報記録再生システムは、以上のように、個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、上記情報記録再生装置に記録すべき情報に上記識別情報を付加する識別情報付加手段と、再生すべき情報に付加された識別情報と、該識別情報が付加された情報の再生に用いられる情報記録再生装置の識別情報とが一致するか否かを判断する判断手段とを備えた構成である。

【0218】それゆえ、識別情報を用いて情報記録再生装置を特定して、情報の記録および再生を行うことができる。このため、違法にコピーされた情報の再生を防止することにより、不正な使用を防止して情報を保護することができるという効果を奏する。

【0219】本発明の情報記録再生システムは、以上のように、個々の情報記録再生装置に固有の物理的情報を検出する物理的情報検出手段と、上記物理的情報検出手段により検出された物理的情報を用いて、個々の情報記録再生装置を識別するための識別情報を生成する識別情報生成手段と、情報を記録する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、記録すべき情報を暗号化する暗号化手段と、暗号化された情報を再生する情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて、該暗号化された情報を復号する復号手段とを備えた構成である。

【0220】それゆえ、識別情報を用いて情報記録再生装置を特定して、情報の暗号化および復号を行うことができる。これにより、違法にコピーされた情報の再生を防止することにより、不正な使用を防止して情報を保護することができるという効果を奏する。

【0221】本発明の情報記録再生システムは、以上のように、上記識別情報生成手段は、識別情報を生成するための情報として、上記物理的情報検出手段により検出された物理的情報と、上記情報記録再生装置の装置仕様情報とを用いる構成である。

【0222】それゆえ、情報記録再生装置本体の装置仕様情報を用いて識別情報を生成することができる。このため、より独立性の高い識別情報を生成することができるという効果を奏する。

【0223】本発明の情報配信方法は、以上のように、情報記録再生装置に固有の物理的情報を用いて生成された識別情報を配信すべき情報に付加し、該識別情報が付加された情報を上記情報記録再生装置に配信する構成である。

【0224】上記の構成により、情報が記録される情報記録再生装置の識別情報と配信すべき情報とを関連付けることができる。これにより、保護機能を付加した情報として、情報を配信することができるため、不正に複製された情報が再生されることを防止することにより、不正な使用を防止して情報を保護することができるという

効果を奏する。

【０２２５】本発明の情報配信方法は、以上のように、情報記録再生装置に固有の物理的情報を用いて生成された識別情報を用いて配信すべき情報を暗号化し、該暗号化された情報を上記情報記録再生装置に配信する構成である。

【０２２６】それゆえ、適法に情報が記録された情報記録再生装置の識別情報と記録すべき情報とを関連付けることができる。

【０２２７】すなわち、配信する情報を格納する情報記録再生装置の識別情報を取得することにより該情報記録再生装置を特定することができる。そして、情報を配信する際に、情報を記録する情報記録再生装置に固有の物理的情報を用いて識別情報を生成し、該識別情報を暗号鍵として使用して、上記情報を暗号化して配信することができる。これにより、不正な使用を防止して情報を保護することができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の実施の形態１におけるセキュリティデバイスの概略の構成を示すブロック図である。

【図２】本発明の実施の形態１におけるユーザ情報入力部を備えたセキュリティデバイスの概略の構成を示すブロック図である。

【図３】本発明の実施の形態１におけるセキュリティデバイスの外観を示す図であり、（ａ）は底面図であり、（ｂ）は側面図であり、（ｃ）は平面図である。

【図４】ハードディスクドライブの概略の構成を説明する図であり、（ａ）は斜視図であり、（ｂ）はａ－ａ’矢視断面図である。

【図５】ハードディスクドライブの磁気ディスクの状態を説明する図であり、（ａ）はディスク外径中心とディスク内径中心との関係をを説明する図であり、（ｂ）はディスク外径中心とスピンドルモータの回転中心との関係を説明する図である。

【図６】ハードディスクドライブに搭載されているスピンドルモータの回転駆動系の構造を説明する図である。

【図７】ハードディスクドライブに搭載されているスピンドルモータを回転駆動するための駆動電流の状態と、駆動電流により発生するスパイクノイズとを説明する図である。

【図８】本発明の実施の形態１における物理的情報センサからの出力波形と物理的情報抽出回路からの出力波形、並びに時間軸情報センサからの出力波形と時間軸情報抽出回路からの出力波形を説明する図である。

【図９】本発明の実施の形態１におけるセキュリティデバイスから出力される識別情報のフォーマットの一例を説明する図である。

【図１０】本発明の実施の形態１における情報記録再生装置に対して加速度を与えるための加振部を備えたセキュリティデバイスの概略の構成を示すブロック図である。

【図１１】本発明の実施の形態１におけるセキュリティデバイスをハードディスクドライブに取り付けた状態を説明する側面図である。

【図１２】本発明の実施の形態２における識別情報を付加して情報を保護する情報保護方法を説明する図である。

【図１３】本発明の実施の形態２における識別情報により情報を暗号化し、同じ識別情報にて情報を復号することで情報を保護する情報保護方法を説明する図である。

【図１４】本発明の実施の形態３におけるセキュリティデバイスを搭載した情報の保護機能を有する情報記録再生システムの構成を説明する図である。

【図１５】本発明の実施の形態３におけるセキュリティデバイスからの識別情報とハードディスクドライブからの装置仕様情報とから更に個別化を向上させた情報を得る方法を説明する図である。

【図１６】本発明の実施の形態４におけるセキュリティデバイスからの識別情報を配信情報に付加してユーザに配信する情報配信方法を説明する図である。

【図１７】本発明の実施の形態４におけるセキュリティデバイスからの識別情報を配信情報に付加してユーザに配信する情報配信方法を説明するフローチャートである。

【図１８】本発明の実施の形態４におけるセキュリティデバイスからの識別情報を暗号鍵として配信情報を暗号化してユーザに配信する情報配信方法を説明する図である。

【図１９】本発明の実施の形態４におけるセキュリティデバイスからの識別情報を暗号鍵として配信情報を暗号化してユーザに配信する情報配信方法を説明するフローチャートである。

【図２０】本発明の実施の形態４におけるユーザシステムが複数の情報記録再生装置を有している場合の配信情報方法を説明する図である。

【符号の説明】

１　セキュリティデバイス
２　物理的情報センサ（物理的情報検出手段）
３　時間軸情報センサ
４　物理的情報抽出回路（識別情報生成手段）
５　時間軸情報抽出回路（識別情報生成手段）
６　識別情報生成回路（識別情報生成手段）
７　ユーザ情報入力部
８　信号処理部（識別情報生成手段）
９　センサ部
１３　スピンドルモータ（回転駆動手段）
２０　電機子（回転駆動手段）
２７　加振部（印加部）
３０　識別情報付加手段
３１　情報記録再生装置

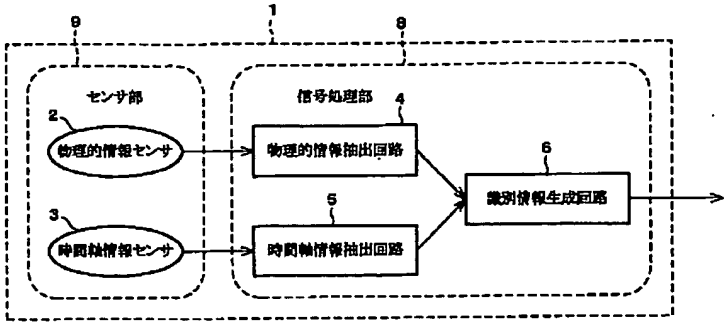
39

３２　認証手段（判断手段）
３３　暗号化手段
３４　復号手段
４１　ＩＤＥ
４６　情報記録再生装置

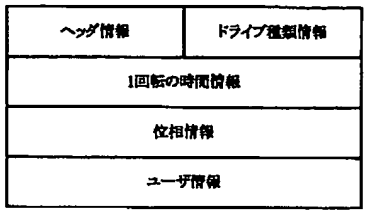
40

＊４７　情報記録再生装置
５２　ＨＤＤ（情報記録再生装置）
６１　セキュリティデバイス
７１　セキュリティデバイス
＊

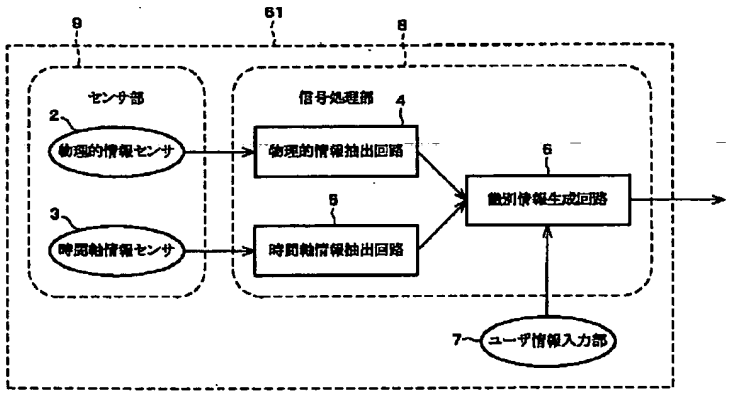
【図１】



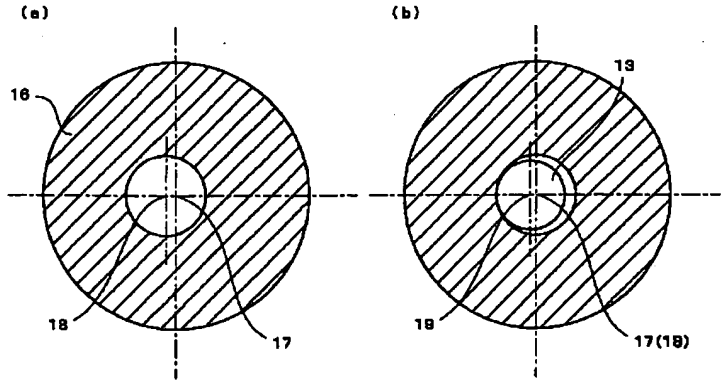
【図９】



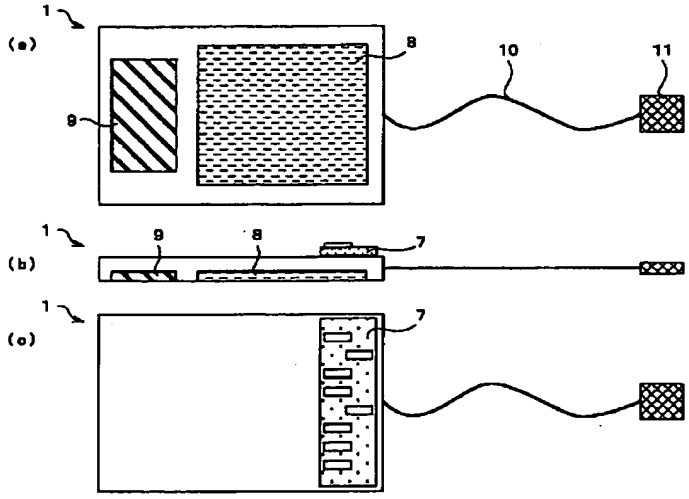
【図２】



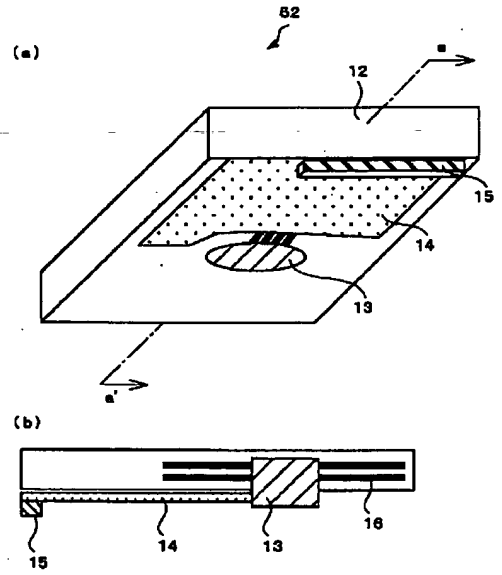
【図５】



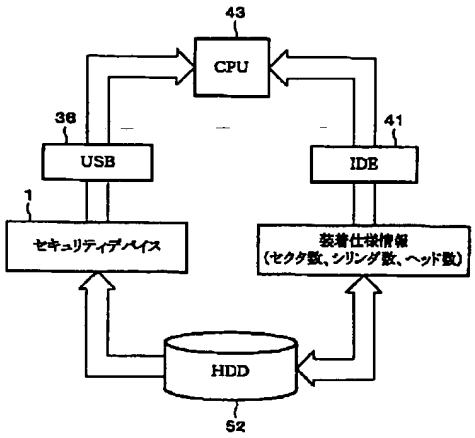
【図3】


1
(a)
8
10
11
9
1
9
8
7
(b)
1
7
(c)

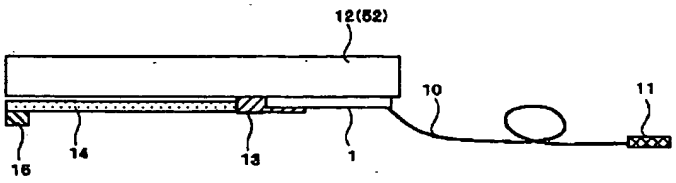
【図4】


52
(a)
12
15
14
13
a'
(b)
16
15
14
13

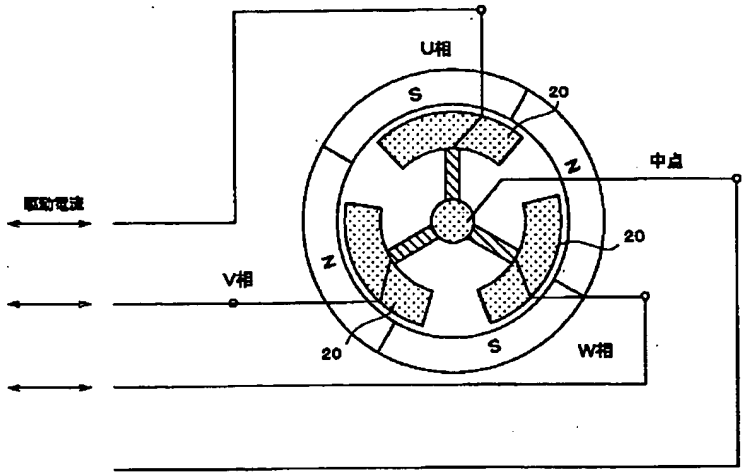
【図15】


43
CPU
36
41
USB
IDE
1
セキュリティデバイス
装着仕様情報
(セクタ数、シリンダ数、ヘッド数)
HDD
52

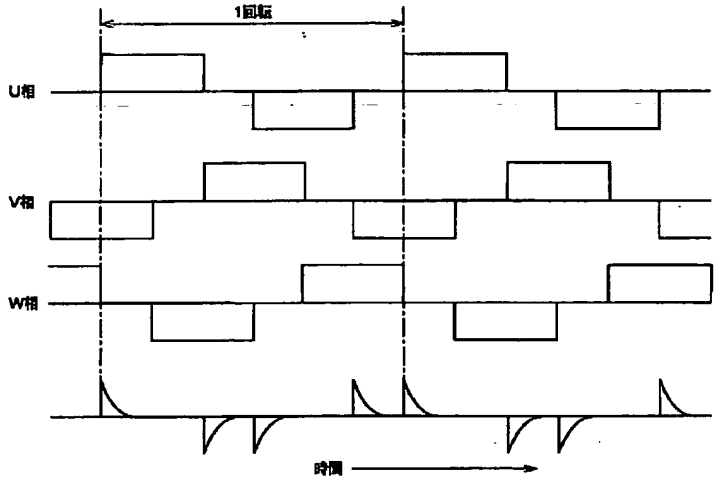
【図11】


12(52)
10
11
16
14
13
1

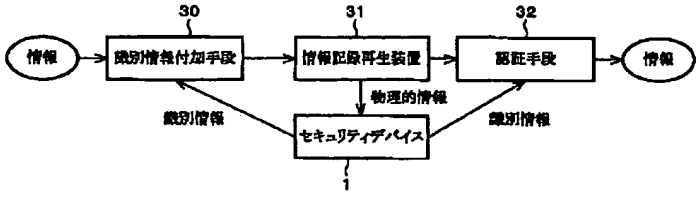
【図6】


U相
S
20
N
中点
駆動電流
20
N
V相
20
S
W相

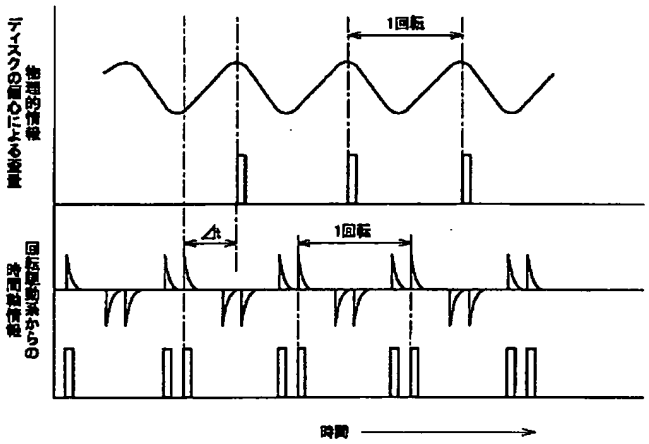
【図7】


1回転
U相
V相
W相
時間

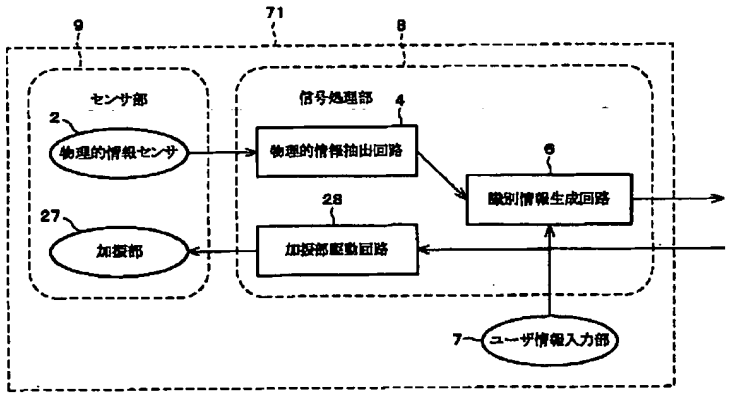
【図12】


30
31
32
情報
識別情報付加手段
情報記録再生装置
認証手段
情報
物理的情報
識別情報
識別情報
セキュリティデバイス
1

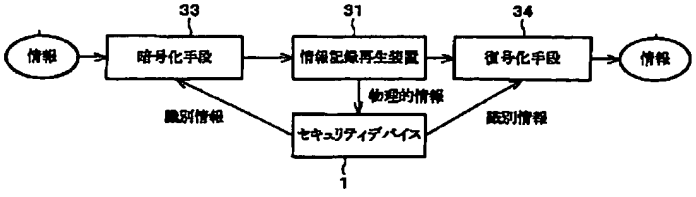
【図８】


ディスクの偏心による変調
物理的情報
1回転
Δt
1回転
回転駆動系からの
時間情報
時間

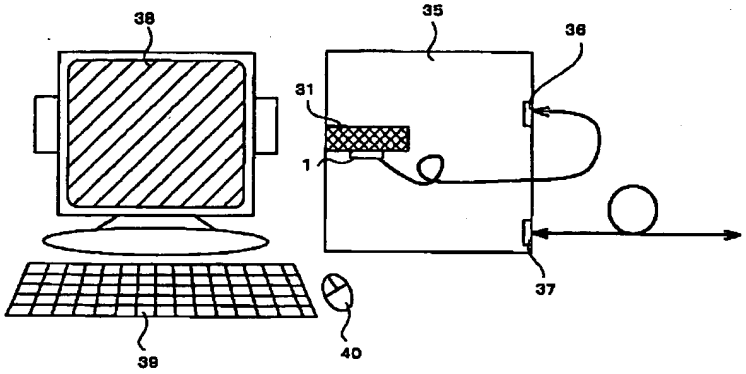
【図１０】


9
71
8
センサ部
2
物理的情報センサ
27
加振部
信号処理部
4
物理的情報抽出回路
28
加振部駆動回路
6
識別情報生成回路
7
ユーザ情報入力部

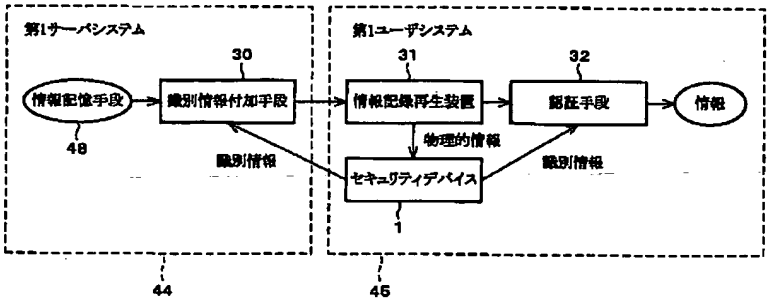
【図１３】


33
31
34
情報
暗号化手段
情報記録再生装置
復号化手段
情報
物理的情報
識別情報
識別情報
セキュリティデバイス
1

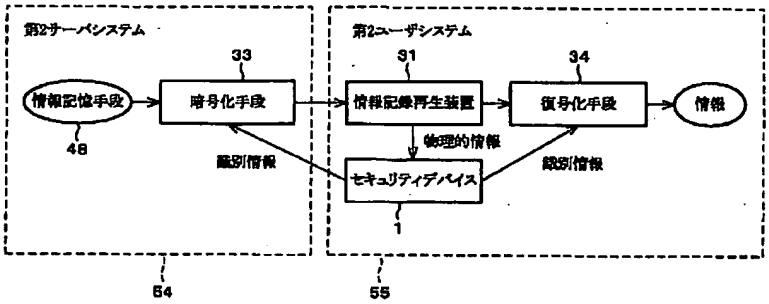
【図１４】


38
35
36
31
1
37
39
40

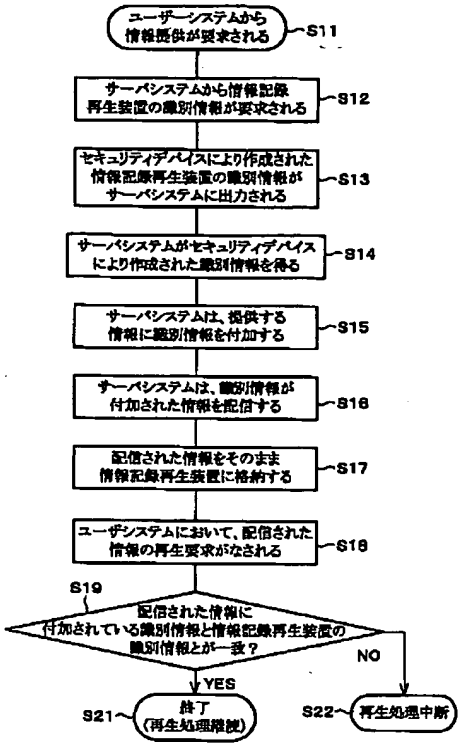
【図１６】


第1サーバシステム
第1ユーザシステム
30
31
32
情報記憶手段
識別情報付加手段
情報記録再生装置
認証手段
情報
物理的情報
識別情報
識別情報
セキュリティデバイス
48
1
44
45

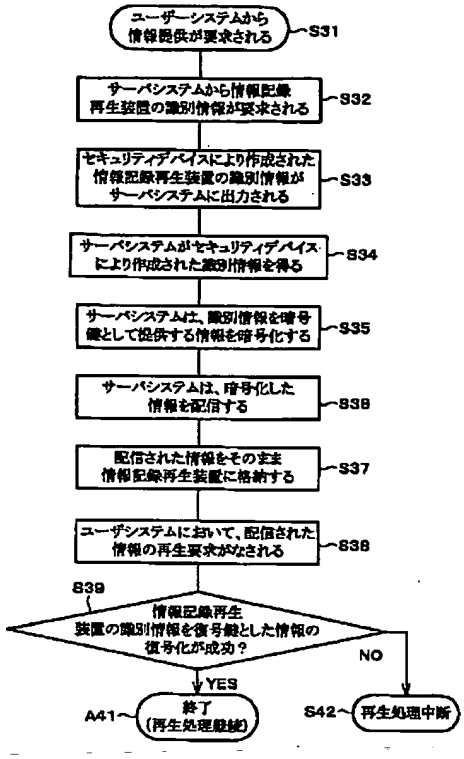
【図１８】


第2サーバシステム
第2ユーザシステム
33
31
34
情報記憶手段
暗号化手段
情報記録再生装置
復号化手段
情報
物理的情報
識別情報
識別情報
セキュリティデバイス
48
1
54
55

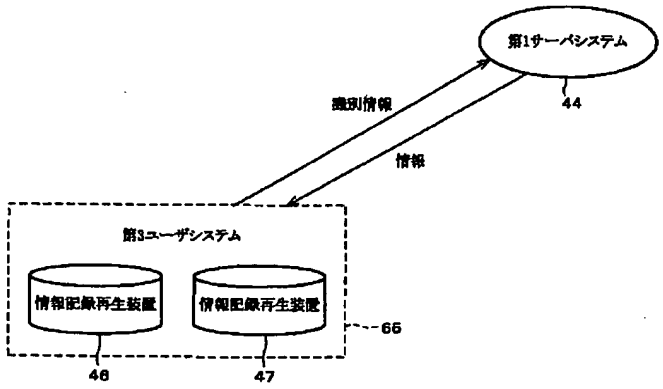
【図１７】



【図１９】



【図２０】



フロントページの続き

(72)発明者　太田　賢司
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

Ｆターム(参考) 5B017 AA07 BA07 BB03 CA16
5D044 AB02 BC08 CC04 CC08 EF05
FG18 GK12 GK17 HH13 HL02
HL08
5D091 AA10 BB04 CC01 DD03 FF11
HH02 HH04